

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION
(PCT Rule 61.2)

Date of mailing: 05 April 2001 (05.04.01)	To: Commissioner US Department of Commerce United States Patent and Trademark Office, PCT 2011 South Clark Place Room CP2/5C24 Arlington, VA 22202 ETATS-UNIS D'AMERIQUE in its capacity as elected Office
International application No.: PCT/JP99/05353	Applicant's or agent's file reference: 349900746971
International filing date: 29 September 1999 (29.09.99)	Priority date:
Applicant: MIYAZAKI, Kunihiro et al	

1. The designated Office is hereby notified of its election made:

in the demand filed with the International preliminary Examining Authority on:

08 November 1999 (08.11.99)

in a notice effecting later election filed with the International Bureau on:

2. The election was

was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

RECEIVED
APR 30 2001
Technology Center 2100

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No.: (41-22) 740.14.35	Authorized officer: J. Zahra Telephone No.: (41-22) 338.83.38
---	---

BEST AVAILABLE COPY

67
Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

9/6/2000

Applicant's or agent's file reference 349900746971	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/JP99/05353	International filing date (day/month/year) 29 September 1999 (29.09.99)	Priority date (day/month/year)
International Patent Classification (IPC) or national classification and IPC H04L 9/10, G06F 12/14, G06K 17/00		RECEIVED JAN 14 2002
Applicant HITACHI, LTD.	Technology Center 2100	

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 5 sheets, including this cover sheet.

This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of _____ sheets.

3. This report contains indications relating to the following items:

- I Basis of the report
- II Priority
- III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV Lack of unity of invention
- V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI Certain documents cited
- VII Certain defects in the international application
- VIII Certain observations on the international application

Date of submission of the demand 08 November 1999 (08.11.99)	Date of completion of this report 13 September 2000 (13.09.2000)
Name and mailing address of the IPEA/JP	Authorized officer
Facsimile No.	Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/JP99/05353

I. Basis of the report

1. With regard to the elements of the international application:^{*} the international application as originally filed the description:pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____ the claims:pages _____, as originally filed
pages _____, as amended (together with any statement under Article 19)
pages _____, filed with the demand
pages _____, filed with the letter of _____ the drawings:pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____ the sequence listing part of the description:pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

2. With regard to the language, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language _____ which is:

 the language of a translation furnished for the purposes of international search (under Rule 23.1(b)). the language of publication of the international application (under Rule 48.3(b)). the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any nucleotide and/or amino acid sequence disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

 contained in the international application in written form. filed together with the international application in computer readable form. furnished subsequently to this Authority in written form. furnished subsequently to this Authority in computer readable form. The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished. The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.4. The amendments have resulted in the cancellation of: the description, pages _____ the claims, Nos. _____ the drawings, sheets/fig _____5. This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).^{**}

* Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).

** Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/JP99/05353

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	3,5,8,9	YES
	Claims	1,2,4,6,7	NO
Inventive step (IS)	Claims		YES
	Claims	1-9	NO
Industrial applicability (IA)	Claims	1-9	YES
	Claims		NO

2. Citations and explanations

Claims 1 and 2

Document 1 [Bruce Schneier, *Applied Cryptography* (Second Edition), John Wiley & Sons, Inc. ed. (1996), "3.7 Secret Sharing," pp. 71-73] describes a decentralized secret sharing method, wherein secret information is decentralized and shared and the secret information can be restored by bringing together decentralized secrets there-among which have a value at least as large as a prescribed threshold value. It is obvious that identical processing results are obtained when data is processed using said secret information as when data is processed using the information obtained by bringing together those decentralized secrets having a value at least as large as the aforementioned prescribed threshold value.

Claims 4, 6, and 7

Document 2 [JP, 10-282881, A (Nippon Telegraph and Telephone Corp.), 23 October 1998 (23.10.98), full text, Figs. 1 to 7] describes the idea of using Shamir's polynomial interpolation to decentralize the secret key of a published key encoding technology into a plurality of parts, registering the same, and using the decentralized information that corresponds to a decentralization threshold value to conduct the data processing when data processing requires the secret key to be restored. The constituent features are the same as the constituent features of the inventions described in claims 4, 6, and 7.

Claims 3, 5, 8, and 9

Document 3 [JP, 3-76447, A (Sharp Corp.), 2 April 1991 (02.04.91), page 3, lower right column, lines 1 to 6; page 3, lower right column, line 13 to page 4, upper left column, line 4; page 4, upper right column, lines 7 to 18; Figs. 1 to 5] describes a technology for securing the secrecy of communications by changing the setting value of the encoding key for each communication.

Document 4 [Kazuo Takaragi, et al., "Sosetsu Shou Tokushuu 'Card' Card Shakai to Security Gijutsu," Nippon Insatsu Gakkaishi, Vol. 29, No. 3, (No. 113) (31.05.92) pp.288-295] suggests the technical viewpoint that it is feasible to have an unlawful-act prevention technology comprising an IC card, wherein the IC card is connected to a reader/writer, the data flowing there-between is acquired, and a card having identical response is made.

Document 5 [Yuichi Kaji, et al., "Password Jizen Sengen ni yoru Kojin Ninshouhou; Jiki Card wo Mochiita Anzenna Kojin Ninshouhou," Technical Research Report of the Institute of

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/JP99/05353

Supplemental Box

(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of Box V (Citations and explanations):

Electronics, Information, and Communication Engineers (ISEC95-39-44), Vol. 95, No. 423 (15.12.95), pp. 21-28] describes a personal identification processing system comprising a card that uses a secret decentralization/sharing technique, the system serving as a safe method for networks.

The technologies described in each of these documents relate to providing protection from unlawful acts committed by persons with malicious intent. It would have been obvious to one skilled in the art to focus on the technical viewpoint described in document 4 and use the card system described in document 5 in the technology that results when the technology for changing the encoding key setting value described in document 3 is applied to the technologies described in documents 1 and 2.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/JP99/05353

VI. Certain documents cited**1. Certain published documents (Rule 70.10)**

Application No. Patent No.	Publication date (day/month/year)	Filing date (day/month/year)	Priority date (valid claim) (day/month/year)
JP,11-316542,A	16 November 1999 (16.11.1999)	04 March 1999 (04.03.1999)	05 March 1998 (05.03.1998)

[E,X]

2. Non-written disclosures (Rule 70.9)

Kind of non-written disclosure	Date of non-written disclosure (day/month/year)	Date of written disclosure referring to non-written disclosure (day/month/year)
--------------------------------	--	---

8709/622371
37C2

PCT
国際予備審査報告

(法第12条、法施行規則第56条)
(PCT36条及びPCT規則70)

特許協力条約

RECEIVED
MAY 9 - 2001
Technology Center 2100

REC'D 03 OCT 2000
WIPO PCT

出願人又は代理人 の書類記号 349900746971	今後の手続きについては、国際予備審査報告の送付通知（様式PCT/IPEA/416）を参照すること。	
国際出願番号 PCT/JP99/05353	国際出願日 (日.月.年) 29.09.99	優先日 (日.月.年)
国際特許分類 (IPC) Int. C17 H04L9/10, G06F12/14, G06K17/00		
出願人 (氏名又は名称) 株式会社日立製作所		

1. 国際予備審査機関が作成したこの国際予備審査報告を法施行規則第57条 (PCT36条) の規定に従い送付する。
2. この国際予備審査報告は、この表紙を含めて全部で <u>5</u> ページからなる。
<input type="checkbox"/> この国際予備審査報告には、附属書類、つまり補正されて、この報告の基礎とされた及び／又はこの国際予備審査機関に対しても訂正を含む明細書、請求の範囲及び／又は図面も添付されている。 (PCT規則70.16及びPCT実施細則第607号参照) この附属書類は、全部で <u> </u> ページである。
3. この国際予備審査報告は、次の内容を含む。
<p>I <input checked="" type="checkbox"/> 国際予備審査報告の基礎</p> <p>II <input type="checkbox"/> 優先権</p> <p>III <input type="checkbox"/> 新規性、進歩性又は産業上の利用可能性についての国際予備審査報告の不作成</p> <p>IV <input type="checkbox"/> 発明の単一性の欠如</p> <p>V <input checked="" type="checkbox"/> PCT35条(2)に規定する新規性、進歩性又は産業上の利用可能性についての見解、それを裏付けるための文献及び説明</p> <p>VI <input checked="" type="checkbox"/> ある種の引用文献</p> <p>VII <input type="checkbox"/> 国際出願の不備</p> <p>VIII <input type="checkbox"/> 国際出願に対する意見</p>

国際予備審査の請求書を受理した日 08.11.99	国際予備審査報告を作成した日 13.09.00
名称及びあて先 日本国特許庁 (IPEA/JP) 郵便番号 100-8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官 (権限のある職員) 青木 重徳 電話番号 03-3581-1101 内線 3574
	5W 4229

I. 国際予備審査報告の基礎

1. この国際予備審査報告は下記の出願書類に基づいて作成された。(法第6条(PCT14条)の規定に基づく命令に応答するために提出された差し替え用紙は、この報告書において「出願時」とし、本報告書には添付しない。PCT規則70.16, 70.17)

 出願時の国際出願書類

<input type="checkbox"/> 明細書	第 _____	ページ、	出願時に提出されたもの
明細書	第 _____	ページ、	国際予備審査の請求書と共に提出されたもの
明細書	第 _____	ページ、	付の書簡と共に提出されたもの
<input type="checkbox"/> 請求の範囲	第 _____	項、	出願時に提出されたもの
請求の範囲	第 _____	項、	PCT19条の規定に基づき補正されたもの
請求の範囲	第 _____	項、	国際予備審査の請求書と共に提出されたもの
請求の範囲	第 _____	項、	付の書簡と共に提出されたもの
<input type="checkbox"/> 図面	第 _____	ページ/図、	出願時に提出されたもの
図面	第 _____	ページ/図、	国際予備審査の請求書と共に提出されたもの
図面	第 _____	ページ/図、	付の書簡と共に提出されたもの
<input type="checkbox"/> 明細書の配列表の部分	第 _____	ページ、	出願時に提出されたもの
明細書の配列表の部分	第 _____	ページ、	国際予備審査の請求書と共に提出されたもの
明細書の配列表の部分	第 _____	ページ、	付の書簡と共に提出されたもの

2. 上記の出願書類の言語は、下記に示す場合を除くほか、この国際出願の言語である。

上記の書類は、下記の言語である _____ 語である。

- 国際調査のために提出されたPCT規則23.1(b)にいう翻訳文の言語
- PCT規則48.3(b)にいう国際公開の言語
- 国際予備審査のために提出されたPCT規則55.2または55.3にいう翻訳文の言語

3. この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際予備審査報告を行った。

- この国際出願に含まれる書面による配列表
- この国際出願と共に提出されたフレキシブルディスクによる配列表
- 出願後に、この国際予備審査（または調査）機関に提出された書面による配列表
- 出願後に、この国際予備審査（または調査）機関に提出されたフレキシブルディスクによる配列表
- 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった
- 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

4. 補正により、下記の書類が削除された。

- 明細書 第 _____ ページ
- 請求の範囲 第 _____ 項
- 図面 図面の第 _____ ページ/図

5. この国際予備審査報告は、補充欄に示したように、補正が出願時における開示の範囲を越えてされたものと認められるので、その補正がされなかったものとして作成した。(PCT規則70.2(c) この補正を含む差し替え用紙は上記1.における判断の際に考慮しなければならず、本報告に添付する。)

V. 新規性、進歩性又は産業上の利用可能性についての法第12条 (PCT35条(2)) に定める見解、それを裏付ける文献及び説明

1. 見解

新規性 (N)	請求の範囲 3, 5, 8, 9 1, 2, 4, 6, 7	有 無
進歩性 (I S)	請求の範囲 1 - 9	有 無
産業上の利用可能性 (I A)	請求の範囲 1 - 9	有 無

2. 文献及び説明 (PCT規則70.7)

請求の範囲 1, 2

文献1 : BRUCE SCHNEIER 著; APPLIED CRYPTOGRAPHY (SECOND EDITION)
John Wiley & Sons, Inc. 発行, (1996)
“3.7 SECRET SHARING”, p. 71-73

には、秘密情報を分散して共有し、そのうちの所定しきい値以上の分散秘密を持ち寄ると、該秘密情報を復元できる分散秘密共有法が記載されており、前記秘密情報によりデータを処理した場合と、前記所定しきい値以上の分散秘密を持ち寄ることで得た情報によりデータを処理した場合とでは得られる処理結果が同一であることは明らかである。

請求の範囲 4, 6, 7

文献2 : JP, 10-282881, A (日本電信電話株式会社)
23. 10月. 1998 (23. 10. 98) 全文, 第1 - 7図
には、公開鍵暗号技術における秘密鍵をShamirの多項式補間法を用いて複数に分散して登録し、データ処理などで前記秘密鍵を復元する必要があるときには分散しきい値に相当する分散情報を用い前記データ処理を実施することが記載されているおり、請求の範囲4, 6, 7に記載されているものと構成が同一である。

請求の範囲 3, 5, 8, 9

文献3 : JP, 3-76447, A (シャープ株式会社)
2. 4月. 1991 (02. 04. 91)
第3頁右下欄第1 - 6行,
第3頁右下欄第13行 - 第4頁左上欄第4行,
第4頁右上欄第7 - 18行, 第1 - 5図

には、暗号鍵の設定値を通信毎に変更することで通信の秘密を確保する技術が記載されている。

文献4 : 宝木和夫, 林義昭; “総説小特集「カード」 カード社会とセキュリティ技術”

日本印刷学会誌, 第29巻, 第3号 (通巻113号)
(31. 05. 92) p. 288 - 295

には、ICカードによる不正防止技術として、ICカードをリーダ/ライタと接続し、その間を流れる情報を入手し、同一応答のカードを作ることが考えられるという技術課題が示唆されている。

文献5 : 桂雄一, 嵩忠雄; “パスワード事前宣言による個人認証法 - 磁気カードを用いた安全な個人認証法”

VI. ある種の引用文献

1. ある種の公表された文書 (PCT規則70.10)

出願番号 特許番号	公知日 (日. 月. 年)	出願日 (日. 月. 年)	優先日 (有効な優先権の主張) (日. 月. 年)
JP, 11-316542, A 「E, X」	16. 11. 99	04. 03. 99	05. 03. 98

2. 書面による開示以外の開示 (PCT規則70.9)

書面による開示以外の開示の種類	書面による開示以外の開示の日付 (日. 月. 年)	書面による開示以外の開示に言及している 書面の日付 (日. 月. 年)

補充欄（いずれかの欄の大きさが足りない場合に使用すること）

第 V. 2 欄の続き

電子情報通信学会技術研究報告 (I S E C 9 5 - 3 9 ~ 4 4)

Vo 1. 95, No. 423 (15. 12. 95) p. 21-28

には、ネットワーク的にも安全な方法として、秘密分散共有の技法を利用したカードによる個人認証の処理システムが記載されている。

そして、各文献に記載されている技術は、共に悪意者による不正からの保護を課題とする技術であるから、文献4に記載されている技術課題に着目し、文献1, 2に記載されている技術に、文献3に記載されている暗号鍵の設定値変更技術を採用したものを、文献5に記載されているカードシステムに使用することは、当業者にとっては自明なことである。

特許協力条約

PCT

E.P

U.S

国際調査報告

(法8条、法施行規則第40、41条)
(PCT18条、PCT規則43、44)

出願人又は代理人 の書類記号 349900746971	今後の手続きについては、国際調査報告の送付通知様式(PCT/ISA/220) 及び下記5を参照すること。	
国際出願番号 PCT/JP99/05353	国際出願日 (日.月.年) 29.09.99	優先日 (日.月.年)
出願人(氏名又は名称) 株式会社日立製作所		

国際調査機関が作成したこの国際調査報告を法施行規則第41条(PCT18条)の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で 3 ページである。

この調査報告に引用された先行技術文献の写しも添付されている。

1. 国際調査報告の基礎

a. 言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。
 この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

b. この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。
 この国際出願に含まれる書面による配列表
 この国際出願と共に提出されたフレキシブルディスクによる配列表
 出願後に、この国際調査機関に提出された書面による配列表
 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表
 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。
 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

2. 請求の範囲の一部の調査ができない(第I欄参照)。

3. 発明の單一性が欠如している(第II欄参照)。

4. 発明の名称は 出願人が提出したものと承認する。

次に示すように国際調査機関が作成した。

5. 要約は 出願人が提出したものと承認する。

第III欄に示されているように、法施行規則第47条(PCT規則38.2(b))の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から1ヶ月以内にこの国際調査機関に意見を提出することができる。

6. 要約書とともに公表される図は、

第 1 図とする。 出願人が示したとおりである。

なし

出願人は図を示さなかった。

本図は発明の特徴を一層よく表している。

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl'

H04L9/10, G06F12/14, G06K17/00

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl'

H04L9/10, G06F12/14, G06K17/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-1999年
日本国登録実用新案公報	1994-1999年
日本国実用新案登録公報	1996-1999年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X Y	BRUCE SCHNEIER 著;APPLIED CRYPTOGRAPHY (SECOND EDITION) John Wiley & Sons, Inc. 発行 (1996), “3.7 SECRET SHARING”, p. 71-73 “3.7 SECRET SHARING”, p. 71-73	1, 2, 4, 6, 7 3, 5, 8, 9
X Y	J P, 10-282881, A (日本電信電話株式会社) 23. 10月. 1998 (23. 10. 98) 全文, 第1-7図 全文, 第1-7図 (ファミリーなし)	1, 2, 4, 6, 7 3, 5, 8, 9

 C欄の続きにも文献が列挙されている。 パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日

27. 12. 99

国際調査報告の発送日

18.01.00

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

青木 重徳

5W 4229



電話番号 03-3581-1101 内線 3576

C (続き) 関連すると認められる文献		関連する 請求の範囲の番号
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	
Y	J P, 3-76447, A (シャープ株式会社) 2. 4月. 1991 (02. 04. 91) 第3頁右下欄第1-6行, 第3頁右下欄第13行-第4頁左上欄第4行, 第4頁右上欄第7-18行, 第1-5図 (ファミリーなし)	3, 5, 8, 9
Y	宝木和夫, 林義昭; “総説小特集「カード」カード社会とセキュリティ技術” 日本印刷学会誌, 第29巻, 第3号, (通巻113号) (31. 05. 92) p. 288-295	1-9
Y	楫雄一, 嵩忠雄; “パスワード事前宣言による個人認証法 -磁気カードを用いた安全な個人認証法” 電子情報通信学会技術研究報告 (I SEC 95-39~44) Vol. 95, No. 423 (15. 12. 95) p. 21-28	1-9
E, X	J P, 11-316542, A (松下電器産業株式会社) 16. 11月. 1999 (16. 11. 99) 全文, 第1-7図 (ファミリーなし)	1-9

特許協力条約に基づく国際出願

願書

出願人は、この国際出願が特許協力条約に従つて処理されることを請求する。

国際出願番号
国際出願日
(受付印)
出願人又は代理人の登録記号 (希望する場合は最大12字) 349900746971

第I欄 発明の名称

秘密情報の処理装置、プログラムまたはシステム

第II欄 出願人

氏名(名称)及びあて名: (姓・名の順に記載; 法人は公式の完全な名称を記載; あて名は郵便番号及び国名も記載)

株式会社 日立製作所
HITACHI, LTD.
〒101-8010 日本国東京都千代田区神田駿河台四丁目6番地
6, Kanda Surugadai 4-chome, Chiyoda-ku,
TOKYO 101-8010 JAPAN

この欄に記載した者は、
発明者である。

電話番号:

ファクシミリ番号:

加入電信番号:

国籍(国名): 日本国 JAPAN

住所(国名): 日本国 JAPAN

この欄に記載した者は、次の
指定国についての出願人である: すべての指定国 レ 米国を除くすべての指定国 米国のみ 追記欄に記載した指定国

第III欄 その他の出願人又は発明者

氏名(名称)及びあて名: (姓・名の順に記載; 法人は公式の完全な名称を記載; あて名は郵便番号及び国名も記載)

宮崎邦彦
✓MITSUYAZAKI Kunihiko
〒215-0013 日本国神奈川県川崎市麻生区王禅寺1099番地
株式会社日立製作所 システム開発研究所
C/O Systems Development Laboratory, HITACHI, LTD.
1099, Ouzenji, Asao-ku, Kawasaki-shi, KANAGAWA
215-0013 JAPAN

この欄に記載した者は、
次に該当する:

出願人のみである。

レ 出願人及び発明者である。

発明者のみである。
(ここにレ印を付したときは、以下に記入しないこと)

国籍(国名): 日本国 JAPAN

住所(国名): 日本国 JAPAN

この欄に記載した者は、次の
指定国についての出願人である: すべての指定国 米国を除くすべての指定国 レ 米国のみ 追記欄に記載した指定国

レ その他の出願人又は発明者が統葉に記載されている。

第IV欄 代理人又は共通の代表者、通知のあて名

次に記載された者は、国際機関において出願人のために行動する:

レ 代理人

共通の代表者

氏名(名称)及びあて名: (姓・名の順に記載; 法人は公式の完全な名称を記載; あて名は郵便番号及び国名も記載)

7509弁理士作田康夫
SAKUTA Yasuo, Patent Attorney (Reg. No. 7509)
〒100-8220 日本国東京都千代田区丸の内一丁目5番1号
株式会社日立製作所内
C/O HITACHI, LTD., 5-1, Marunouchi 1-chome, Chiyoda-ku,
TOKYO 100-8220 JAPAN

電話番号:
03-3212-1111

ファクシミリ番号:
03-3214-3116

加入電信番号:

通知のための宛名: 代理人又は共通の代表者が選任されておらず、上記欄内に特に通知が送付されるあて名を記載している場合は、レ印を付す

第Ⅲ欄の続き その他の出願人又は発明者

この欄を記載しないときは、この用紙を願書に含めないこと。

氏名（名称）及びあて名：（姓・名の順に記載；法人は公式の完全な名称を記載；あて名は郵便番号及び国名も記載）

宝木和夫

TAKARAGI Kazuo

〒215-0013 日本国神奈川県川崎市麻生区王禅寺1099番地

株式会社日立製作所 システム開発研究所内

C/O Systems Development Laboratory, HITACHI, LTD.

1099, Ouzenji, Asao-ku, Kawasaki-shi, KANAGAWA

215-0013 JAPAN

この欄に記載した者は、

次に該当する：

 出願人のみである。 レ 出願人及び発明者である。 発明者のみである。

（ここにレ印を付したときは、以下に記入しないこと）

国籍（国名）： 日本国 JAPAN

住所（国名）： 日本国 JAPAN

この欄に記載した者は、次の
指定国についての出願人である： すべての指定国 米国を除くすべての指定国 レ 米国のみ 追記欄に記載した指定国

氏名（名称）及びあて名：（姓・名の順に記載；法人は公式の完全な名称を記載；あて名は郵便番号及び国名も記載）

福澤寧子

FUKUZAWA Yasuko

〒215-0013 日本国神奈川県川崎市麻生区王禅寺1099番地

株式会社日立製作所 システム開発研究所内

C/O Systems Development Laboratory, HITACHI, LTD.

1099, Ouzenji, Asao-ku, Kawasaki-shi, KANAGAWA

215-0013 JAPAN

この欄に記載した者は、

次に該当する：

 出願人のみである。 レ 出願人及び発明者である。 発明者のみである。

（ここにレ印を付したときは、以下に記入しないこと）

国籍（国名）： 日本国 JAPAN

住所（国名）： 日本国 JAPAN

この欄に記載した者は、次の
指定国についての出願人である： すべての指定国 米国を除くすべての指定国 レ 米国のみ 追記欄に記載した指定国

氏名（名称）及びあて名：（姓・名の順に記載；法人は公式の完全な名称を記載；あて名は郵便番号及び国名も記載）

この欄に記載した者は、

次に該当する：

 出願人のみである。 出願人及び発明者である。 発明者のみである。

（ここにレ印を付したときは、以下に記入しないこと）

国籍（国名）：

住所（国名）：

この欄に記載した者は、次の
指定国についての出願人である： すべての指定国 米国を除くすべての指定国 米国のみ 追記欄に記載した指定国

氏名（名称）及びあて名：（姓・名の順に記載；法人は公式の完全な名称を記載；あて名は郵便番号及び国名も記載）

この欄に記載した者は、

次に該当する：

 出願人のみである。 出願人及び発明者である。 発明者のみである。

（ここにレ印を付したときは、以下に記入しないこと）

国籍（国名）：

住所（国名）：

この欄に記載した者は、次の
指定国についての出願人である： すべての指定国 米国を除くすべての指定国 米国のみ 追記欄に記載した指定国 その他の出願人又は発明者が統表に記載されている。

第V欄　　国の指定

規則 4.9(a)の規定に基づき次の指定を行う(該当する□内にレ印を付すこと;少なくとも1つの□にレ印を付すこと)。

廣域特許

□ A P A R I P O 特許 : G H ガーナ Ghana, K E ケニア Kenya, L S レソト Lesotho, M W マラウイ Malawi, S D スーダン Sudan, S Z スワジランド Swaziland, U G ウガンダ Uganda, Z W ジンバブエ Zimbabwe, 及びハラレプロトコルと特許協力条約の締約国である他の国

□ E A ヨーラシア特許 : A M アルメニア Armenia, A Z アゼルバイジャン Azerbaijan, B Y ベラルーシ Belarus, K G キルギスタン Kyrgyzstan, K Z カザフスタン Kazakhstan, M D モルドバ Republic of Moldova, R U ロシア連邦 Russian Federation, T J タジキスタン Tajikistan, T M トルクmenistan Turkmenistan, 及びヨーラシア特許条約と特許協力条約の締約国である他の国

□ E P ヨーロッパ特許 : A T オーストリア Austria, B E ベルギー Belgium, C H and L I スイス及びリヒテンシュタイン Switzerland and Liechtenstein, C Y キプロス Cyprus, D E ドイツ Germany, D K デンマーク Denmark, E S スペイン Spain, F I フィンランド Finland, F R フランス France, G B 英国 United Kingdom, G R ギリシャ Greece, I E アイルランド Ireland, I T イタリア Italy, L U ルクセンブルグ Luxembourg, M C モナコ Monaco, N L オランダ Netherlands, P T ポルトガル Portugal, S E スウェーデン Sweden, 及びヨーロッパ特許条約と特許協力条約の締約国である他の国

□ O A O A P I 特許 : B F ブルキナ・ファソ Burkina Faso, B J ベニン Benin, C F 中央アフリカ Central African Republic, C G コンゴ Congo, C I 象牙海岸 Cote d'Ivoire, C M カメルーン Cameroon, G A ガボン Gabon, G N ギニア Guinea, M L マリ Mali, M R モーリタニア Mauritania, N E ニジェール Niger, S N セネガル Senegal, T D チャード Chad, T G トーゴ Togo, 及びアフリカ知的所有権機構と特許協力条約の締約国である他の国(他の種類の保護又は取扱いを求める場合には点線に記載する)

国内特許（他の種類の保護又は取扱いを求める場合には点線上に記載する）

A L アルバニア Albania
 A M アルメニア Armenia
 A T オーストリア Austria
 A U オーストラリア Australia
 A Z アゼルバイジャン Azerbaijan
 B A ボスニア・ヘルツェゴビナ Bosnia and Herzegovina

 B B バルバドス Barbados
 B G ブルガリア Bulgaria
 B R ブラジル Brazil
 B Y ベラルーシ Belarus
 C A カナダ Canada
 C H and L I スイス及びリヒテンシュタイン Switzerland and Liechtenstein

 C N 中国 China
 C U キューバ Cuba
 C Z チェコ Czech Republic
 D E ドイツ Germany
 D K デンマーク Denmark
 E E エストニア Estonia
 E S スペイン Spain
 F I フィンランド Finland
 G B 英国 United Kingdom
 G E グルジア Georgia
 G H ガーナ Ghana
 H U ハンガリー Hungary
 I L イスラエル Israel
 I S アイスランド Iceland
 J P 日本 Japan
 K E ケニア Kenya
 K G キルギスタン Kyrgyzstan
 K R 韓国 Republic of Korea
 K Z カザフスタン Kazakstan
 L C セントルシア Saint Lucia
 L K スリ・ランカ Sri Lanka
 L R リベリア Liberia
 L S レソト Lesotho
 L T リトアニア Lithuania
 L U ルクセンブルグ Luxembourg
 L V ラトヴィア Latvia
 M D モルドヴァ Republic of Moldova
 M G マダガスカル Madagascar
 M K マケドニア旧ユーゴスラヴィア The former Yugoslav Republic of Macedonia

<input type="checkbox"/>	M N	モンゴル Mongolia
<input type="checkbox"/>	M W	マラウイ Malawi
<input type="checkbox"/>	M X	メキシコ Mexico
<input type="checkbox"/>	N O	ノールウェー Norway
<input type="checkbox"/>	N Z	ニュージーランド New Zealand
<input type="checkbox"/>	P L	ポーランド Poland
<input type="checkbox"/>	P T	ポルトガル Portugal
<input type="checkbox"/>	R O	ルーマニア Romania
<input type="checkbox"/>	R U	ロシア連邦 Russian Federation
<input type="checkbox"/>	S D	スーダン Sudan
<input type="checkbox"/>	S E	スウェーデン Sweden
<input checked="" type="checkbox"/>	S G	シンガポール Singapore
<input type="checkbox"/>	S I	スロヴェニア Slovenia
<input type="checkbox"/>	S K	スロバキア Slovakia
<input type="checkbox"/>	S L	シェラレオネ Sierra Leone
<input type="checkbox"/>	T J	タジキスタン Tajikistan
<input type="checkbox"/>	T M	トルクメニスタン Turkmenistan
<input type="checkbox"/>	T R	トルコ Turkey
<input type="checkbox"/>	T T	トリニダード・トバゴ Trinidad and Tobago
<input type="checkbox"/>	U A	ウクライナ Ukraine
<input type="checkbox"/>	U G	ウガンダ Uganda
<input checked="" type="checkbox"/>	U S	米国 United States of America
<input type="checkbox"/>	U Z	ウズベキスタン Uzbekistan
<input type="checkbox"/>	V N	ヴィエトナム Viet Nam
<input type="checkbox"/>	Y U	ユーゴスラビア Yugoslavia
<input type="checkbox"/>	Z W	ジンバブエ Zimbabwe

以下の口は、この様式の施行後に特許協力条約の締約国となった国を指定（国内特許のために）するためのものである

出願人は、上記の指定に加えて、規則49(6)の規定に基づき、特許協力条約の下で認められる全ての国の指定を行う。

の國の指定を除く。

ただし、これらの追加される指定が確認を条件としていること、並びに受付日から15月が経過する前にその確認がなされない指定は、この期間の経過時に、出願人によって取り下げられたものとみなされることを宣言する。（指定の確認は、指定を特定する通知の提出と指定手数料及び確認手数料の納付からなる。この確認は、受付日から15月以内に受理官庁へ提出されなければならない。）

第VI欄 優先権主張

 他の優先権の主張（先の出願）が追記欄に記載されている

下記の先の出願に基づき優先権を主張する

元の出願

先の出願の出願日 (日、月、年)	先の出願の出願番号	国内出願：国名	広域出願：*広域官庁名	国際出願：受理官庁名
(1)				
(2)				
(3)				

上記()の番号の先の出願（ただし、本国際出願が提出される受理官庁に対して提出されたものに限る）のうち、次の()の番号のものについては、出願書類の認証原本を作成し国際事務局へ送付することを、受理官庁（日本国特許庁の長官）に対して請求している。

*先の出願が、A.R.I.P.Oの特許出願である場合には、その先の出願を行った工業所有権の保護のためのパリ条約同盟国の中なくとも1ヶ国を追記欄に表示しなければならない（規則4.10(b)(ii)）。追記欄を参照。

第VII欄 國際調査機関

国際調査機関 (ISA) の選択	先の調査結果の利用請求；当該調査の照会 (先の調査が、国際調査機関によって既に実施又は請求されている場合)		
ISA / JP	出願日 (日、月、年)	出願番号	国名 (又は広域官庁)

第VIII欄 照合欄

この国際出願の用紙の枚数は次のとおりである。

顧客	4枚
明細書（配列表を除く）	40枚
請求の範囲	3枚
要約書	1枚
図面	12枚
明細書の配列表	枚
合計	60枚

この国際出願には、以下にチェックした書類が添付されている。

1. 手数料計算用紙
2. 納付する手数料に相当する特許印紙を貼付した書面
3. 國際事務局の口座への振込みを証明する書面
4. 別個の記名押印された委任状
5. 包括委任状の写し
6. 記名押印（署名）の説明書
7. 寄託した微生物又は他の生物材料に関する書面
8. ヌクレオチド又はアミノ酸配列表（フレキシブルディスク）
9. その他（書類名を詳細に記載する）
: 優先権書類送付請求書

要約書とともに提示する図面 第1図

本国際出願の使用言語名： 日本語

第IX欄 提出者の記名押印

各人の氏名（名称）を記載し、その次に押印する。

作田康夫

1. 国際出願として提出された書類の実際の受理の日	受 理 官 庁 記 入 欄		2. 図面
3. 国際出願として提出された書類を補完する書類又は図面であって その後期間内に提出されたものの実際の受理の日（訂正日）			
4. 特許協力条約第11条(2)に基づく必要な補完の期間内の受理の日			
5. 出願人より特定された 国際調査期間			
I S A / J P	6. <input type="checkbox"/> 調査手数料未払いにつき、国際調査機関に調査用写しを送付していない		<input type="checkbox"/> 受理された <input type="checkbox"/> 不足図面がある

国際事務局記入欄

記録原本の受理の日

様式P.C.T./R.O./101 (最終用紙) (1998年7月)

明細書

program system
秘密情報の処理装置、プログラムまたはシステム

技術分野

security

本発明は、情報のセキュリティを確保する技術に関する。

5

背景技術

ICカードは、その構造上、内部に対する情報の読み書きがICカード自身が持つ演算処理部の制御の下で行われるため、磁気カード等と比較して安全に情報を管理することができ、それゆえ、秘密にすべき情報を安全に管理するための手段としての利用が注目されている。今後、例えば、暗号文を復号する機能およびそのために必要な鍵情報をもったICカードや、電子的なデータに対するデジタル署名を生成する機能およびそのために必要な鍵情報をもったICカードなどの利用がさらに広がることが期待されている。

15 public key digital signature
公開鍵やデジタル署名といった誰もが知ることができる情報から、計算によって、秘密鍵を知ることは、計算量的に、非常に困難であり、実際上不可能であることが知られている。

その一方で、ICカードなどの上記暗号化、復号化、署名作成などの機能を持った装置(secure cryptographic device という)に対する新たな脅威として、内部にある重要な情報(例えば秘密鍵)を、物理的に直接解析をすることなく、通常の使用方法における処理時間、消費電流、発生する電磁波等をdeviceの外部から解析することによって、推定しようとするTA(Timing Attack), DPA(Differential Power Analysis), SPA(Simple Power Analysis)などの攻撃法の可能性が示唆されるようになっている。

たとえば、これらの攻撃により、署名作成のための秘密鍵が解析されると、悪意のある人が正当な所有者になりますことが可能になるなど影響が大きく、対策が求められている。

ICカードについては、

5 文献[Handbook] Rankl Effing, "Smart Card Handbook", John Wiley & Sons, 1997

に開示されている。

secure cryptographic deviceについては、

文献[ISO13491] ISO13491-1 "Banking - Secure cryptographic devices (retail) - Part 1: Concepts, requirements and evaluation methods", First edition 1998-06-15

に開示されている。

また、TA(Timing Attack), DPA(Differential Power Analysis), SPA(Simple Power Analysis)などのアタックについては、前記文献 [Handbook]の他、

文献[DPA] Paul Kocher, Joshua Jaffe and Benjamin Jun, "Introduction to Differential Power Analysis and Related Attacks", 1998

文献[TA] Paul Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems", CRYPTO'96, 1996

20 に開示されている。

上記各攻撃法は、間接的に得られる測定結果と内部情報とが相関を持つことを根拠とするものである。

RSA暗号の復号化機能をもつICカードへのTiming Attackに対する対策として、上記文献[TA]には、ブラインド署名という技術を応用した対策案が示されている。これは、Timing Attack を実行する際に必要となるサンプルデータを探りにくくするために、入力として与えられる暗号

文を直接復号するのではなく、暗号文に乱数情報を加えたものを復号し、最後に再び乱数による影響を取り扱うことにより、復号文を得る手法である。しかしながら依然として、あるデータを秘密鍵乗するという処理 ^{raise data to the secret key's power} が含まれている点で充分でない。

5

発明の開示

本発明は、上記課題に鑑みてなされたものであり、ICカード等の *secure cryptographic device* 内の秘密情報を推定できないようにする手段、技術を提供することを目的とする

10 すなわち、本発明は、ICカード等の *secure cryptographic device* に対する TA(Timing Attack), DPA(Differential Power Analysis), SPA(Simple Power Analysis) 等の攻撃法を無効とする手段、技術を提供することを目的とする。

15 さらに、これらの手段、技術を利用した ICカード、セキュリティモジュール、半導体チップ、システム、コンピュータ、プログラムを提供することを目的としている。

上記目的を達成するために、本発明は、演算処理回路と記憶回路とそれらを接続する信号線とで構成した秘密情報の処理装置において、秘密情報と処理対象となるデータとを既知の処理方法に基づいて処理した処理結果と同一の処理結果を得るように構成された秘密情報の処理方法であって、上記秘密情報とは異なる秘密情報生成情報と、上記秘密情報生成情報と上記処理対象となるデータとを用い同一の上記処理結果を出力する秘密情報生成情報処理手段とを用いることを特徴とするものである。

さらに、本発明の秘密情報生成情報処理手段は、上記秘密情報を上記演算処理回路や上記記憶回路や上記信号線に出現させることなく処理を行うことを特徴とするものである。

具体的な一例としては、秘密情報は、暗号文の復号や署名生成のための秘密鍵であり、秘密情報処理手段は、暗号化または署名生成の既知アルゴリズムを実現する手段であり、処理結果は、復号化された平文や生成された署名である。秘密鍵とは異なる秘密情報生成情報と、それを用いて、平文や署名を処理結果として出力する秘密情報生成情報処理手段とを用いることにより、秘密情報を外部から知ることが困難になる。
5

さらに、本発明は、同一の秘密情報生成情報処理手段が処理する秘密情報生成情報は、取りうる値が複数あるように構成する。

具体的には、本発明の上記記憶回路は、上記秘密情報生成情報を、その組み合わせが複数ある、複数の秘密情報部分情報として構成し、上記記憶回路に保持することを特徴とするものである。
10

これらの手段を採用することにより、秘密情報そのものは、内部の記憶手段に保持されているときや、記憶手段と演算手段との間を装置内部の信号線(内部バス)を介して送られるとき、演算手段において、上記処理手段によって処理されるとき、いずれの場合においても、出現することが無い。したがって秘密情報をそのものを得ることが困難になる。さらに、秘密情報生成情報は、それと組み合わせて用いる秘密情報生成情報処理手段によって所望の結果を得ることができるので、当該情報だけを得たとしても秘密情報を得たことにはならない。さらに、不正に秘密情報を入手しようとする攻撃者が秘密情報生成情報処理手段を知ったとしても、秘密情報生成情報として取りうるデータが複数通りある時には、攻撃者にとって必要な試行回数が増加するため、秘密情報を得ることがさらに困難になる。
15
20

したがって、かかる時間、発生する電磁波の強さおよび消費電流等から秘密情報そのものを得ることが困難になる。
25

また、上記目的を達成するために、間接的に得られる測定結果と内部

情報との相関関係を少なくする手段を設ける。

より具体的には、本発明では次の手段を用いる。

(1)秘密裏に保持すべき情報を利用した演算において、前記情報を表す複数の表現を演算ごとに使い分ける

5 (2)ある表現方法で記憶装置内に保持された秘密にすべき情報を、その情報を利用した演算が行われる度に、あるいは、あらかじめ決められた時期に、あるいは、ランダムに決められた時期に、別の表現に変換し、変換された新たな表現により元の表現を書き換える

(3)秘密裏に保持すべき情報Aとそれとは異なる情報Bを利用した演算において、前記情報Bを表す複数の表現を演算ごとに使い分ける

(4)秘密にすべき情報Aを利用した演算に使われる情報であって、ある表現方法で記憶装置内に保持された前記秘密にすべき情報Aとは異なる情報Bを、前記秘密にすべき情報Aを利用した演算が行われる度に、あるいは、あらかじめ決められた時期に、あるいは、ランダムに決められた時期に、別の表現に変換し、変換された新たな表現により元の表現を書き換える

すなわち、本発明の上記記憶回路は、上記秘密情報生成情報を他の秘密情報生成情報へ変換する変換手段をさらに備え、上記他の秘密情報生成情報は、上記秘密情報生成情報処理手段が上記処理結果と同一の処理結果を出力させる情報であることを特徴とするものである。

さらに、本発明の上記演算処理回路は、上記変換手段を、所定の時期に実行することを特徴とするものである。

上記手段を採用することにより、前記秘密にすべき情報Aを利用する演算が実行される際にかかる時間、発生する電磁波の強さおよび消費電流等が、一定にならないようにし、結果として、前記前記秘密にすべき情報Aと、情報Aを利用する演算にかかる時間、発生する電磁波の強さおよ

び消費電流との間の関連(相関関係)を少なくする。

なお、上記秘密情報生成情報処理手段や変換手段は、具体的な一例としては、プログラムであり、ディジタル信号処理プロセッサ(DSPという)、中央演算処理回路(CPUという)などの演算手段によって実行されるものである。

5

また、本発明は、上述の秘密情報の処理装置を用いて、上記秘密情報を用いた処理結果を送受信する秘密情報の処理システムであって、上記処理結果の受信者側装置は、上記秘密情報生成情報処理手段と上記秘密情報生成情報とを、上記処理装置の上記記憶回路に設定する手段を備え、
10 处理装置の使用者側装置は、上記処理装置に処理対象となるデータを入力する手段と、上記処理装置から上記処理結果を受け取る手段と、上記受け取った処理結果を上記受信者側装置へ送信する手段とを備えることを特徴とするものである。

15 図面の簡単な説明

第1図は、本発明の一実施例におけるICカード構成図であり、第2図は、第1図のICカード構成のうち表現変換プログラムのフローであり、第3図は、第1図のICカード構成のうち楕円曲線暗号復号プログラムのフローであり、第4図は、第1図のICカード構成のうち共通鍵暗号復号プログラムのフローであり、第5図は、本発明の一実施例におけるICカード構成図であり、第6図は、第5図のICカード構成のうちテーブルデータ計算プログラムのフローであり、第7図は、第5図のICカード構成のうちテーブル参照型楕円曲線暗号復号プログラムのフローであり、第8図は、本発明の一実施例におけるICカード構成図であり、第9図は、第20
20
25
8図のICカード構成のうち点表現変換プログラムのフローであり、第10図は、本発明の一実施例におけるICカード構成図、第11図は、第1

0 図の ICカード構成のうち ECDSA 署名生成プログラムのフローである。

発明を実施するための最良の形態

・第 1 の実施例

5 本発明を、 楕円曲線暗号の一種である Elliptic Curve Encryption Scheme (ECES) の復号化機能を持った ICカードに適用した一実施例を、 以下、 図を用いて説明する。 Elliptic Curve Encryption Scheme については、 文献[X9.63]に述べられている。

椭円曲線暗号については、

10 文献[X9.63] "Working Draft: AMERICAN NATIONAL STANDARD X9.63-199x Public Key Cryptography For The Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography", American National Standards Institute, January 9, 1999

文献[IEEEP1363] "Standard Specifications For Public Key Cryptography (Draft Version 9)" IEEE P1363 Standard, IEEE, February 8, 1999

に開示されている。

なお、 本実施例において、 上記秘密裏に保存すべき情報(秘密情報)に該当する情報は、 楕円曲線暗号の復号に利用される秘密鍵である。 また 20 本実施例では、 素数位数の有限体上の椭円曲線を利用するものとする。

第 1 図は、 本実施例における ICカードのハードウェア構成図である。 ICカード 1001 は、 CPU 等で構成する演算処理部 1002、 記憶回路(メモリ)で構成するデータ格納部 1004 とプログラム格納部 1005、 インターフェイス回路で構成する I/O 1006、 およびこれら各構成要素を内部で接続するバス 25 1003 とからなる。

プログラム格納部 1005 には、 表現変換プログラム 1010 と、 楕円曲線暗

号復号プログラム1011と、共通鍵暗号復号プログラム1012が保存されており、それぞれ、演算処理部1002に読み出され、実行される。

データ格納部1004には、楕円曲線暗号におけるシステム鍵1009が保存されている。システム鍵は、楕円曲線暗号で利用する楕円曲線を決めるためのデータであり、あらかじめ、暗号化されたメッセージのやり取りに携わるシステム全体に対し、共通な値として、公開されている。システム鍵は次のような値を含む。すなわち、楕円曲線の定義式 $y^2 = x^3 + ax + b$ の係数aおよびb、前記楕円曲線の定義される有限体の位数p、ベースポイントと呼ばれる前記楕円曲線上の固定された点Pの座標、前記ベースポイントPの位数n、 $n \times h$ が前記楕円曲線上の有理点の個数と等しくなるようなコファクターと呼ばれる数h、を含む。

またデータ格納部1004には、さらに、楕円曲線暗号の復号に利用される秘密鍵dを表すデータ(秘密情報生成情報)が保存されている。ここで特徴的なことは、秘密鍵dそのものがデータ格納部に保存されているわけではない、ということである。本実施例においては、秘密情報生成部分情報である秘密鍵部分情報 d_A 1007と秘密鍵部分情報 d_B 1008の組により、秘密情報生成情報が表現されている。より具体的には、 d_A 1007と d_B 1008の法nにおける差が秘密鍵dの値と等しくなるようになっていて、さらに秘密情報生成情報処理手段に相当する楕円曲線暗号復号プログラム1011は、これらを正しく処理できるように構成されている。 d_A 1007と d_B 1008の組み合わせは複数あり、例えば、 d_A 1007の値を秘密鍵dそのものの値とし、 d_B 1008の値を0(ゼロ)とすれば、この d_A 1007と d_B 1008の組は、秘密鍵dの表現の一例となる。また、 d_A 1007の値を0(ゼロ)とし、 d_B 1008の値を $n - d$ ($\bmod n$) とすれば、これも秘密鍵dの前記とは異なる表現の一例となる。

以下、各プログラムの動作の概略を説明する。

まず、楕円曲線暗号復号プログラム1011による、楕円曲線暗号の復号

処理について説明する。楕円曲線暗号プログラム1011は、データ格納部1004に保存されたシステム鍵1009によって決定される楕円曲線上の演算を含むプログラムであり、ICカード1001の外部から入力として与えられた復号用点R1013、および、データ格納部1004に保存された秘密鍵を表す情報、すなわち本実施例においては、秘密鍵dを求めることなく、秘密鍵情報の一表現である秘密鍵部分情報d_a1007と秘密鍵部分情報d_b1008から、楕円曲線上の点 dR を計算し、暗号化されたメッセージm1014を共通鍵暗号プログラム1012で復号するために必要となる復号用共通鍵を計算するプログラムである。このプログラムの出力として得られた復号用共通鍵は、共通鍵暗号プログラム1012の入力の一部となる。

次に、共通鍵暗号復号プログラム1012による、暗号メッセージの復号処理について説明する。共通鍵暗号復号プログラム1012は、楕円曲線暗号復号プログラム1011の出力として得られた復号用共通鍵およびICカード1001の外部から入力として与えられた暗号化されたメッセージm1014を入力とし、暗号化されたメッセージm1014を復号し、その結果をICカード1001の外部へ、復号化されたメッセージm'1015として出力するプログラムである。

なお、本実施例においては、共通鍵暗号復号プログラム1012による共通鍵暗号処理はICカード1001内で行うものとしたが、この処理はICカード1001と情報のやり取りができる外部の装置、例えば、ICカード1001とICカードリーダライタを通じて情報のやり取りができるPC等で行ってもよい。この場合は、ICカード1001に対する入力は、復号用点R1013となり、ICカード1001からの出力は、楕円曲線暗号復号プログラムの出力である復号用共通鍵となる。

ICカード1001を使った時の暗号化されたメッセージm1014を復号する時の、上記の3つのプログラムによる基本的な動作の流れをまとめると

次のようになる。

まず、楕円曲線暗号復号プログラム1011が、ICカード1001の外部からの入力である復号用点R1013と、データ格納部1004に保存された秘密鍵部分情報d_A1007と秘密鍵部分情報d_B1008から、秘密鍵情報dを求めることなく復号用共通鍵を計算する。次に共通鍵暗号復号プログラム1012が、楕円曲線暗号復号プログラム1011によって計算された復号用共通鍵を使って、ICカード1001の外部からの入力である暗号化されたメッセージm1014を復号し、復号化されたメッセージm'1015として出力する。

これにより、暗号化されたメッセージmを復号することができる。

このように秘密鍵dがデータ格納部1004、バス1003、演算処理部1002に出現することなく暗号化されたメッセージmを復号することができるので、TA(Timing Attack), DPA(Differential Power Analysis), SPA(Simple Power Analysis)等によって秘密鍵の値を推定することが困難になっている。

この例では、データ格納部1004に保存された秘密鍵部分情報d_A1007と秘密鍵部分情報d_B1008の値が固定されている。したがって、復号を行うたびに、固定値である秘密鍵部分情報d_A1007と秘密鍵部分情報d_B1008がデータ格納部1004からバス1003を介して演算処理部1002に毎回流れることになり、また、楕円曲線暗号復号プログラム1011は、毎回同じ計算を行うことになるため、この間の計算時間や発生する電磁波の強さや消費電流等も同じになる。このことはTA(Timing Attack), DPA(Differential Power Analysis), SPA(Simple Power Analysis)等によって秘密鍵部分情報の値を推定される可能性があることを意味する。

本発明では、これらの攻撃に対するさらなる対策として、表現変換プログラム1010を利用する。

表現変換プログラム1010による、秘密鍵情報の表現の変換処理について

て説明する。表現変換プログラム1010は、データ格納部1004から読み出された秘密鍵情報の一表現を、別表現に変換し、この新たな表現を、データ格納部1004中の元の表現と置き換える(書き換える)プログラムである。本実施例においては、表現変換プログラム1010は、データ格納部1004から読み出された秘密鍵情報の一表現である秘密鍵部分情報 d_A 1007と秘密鍵部分情報 d_B 1008の組から、あらたに別の表現、秘密鍵部分情報 d_A' と秘密鍵部分情報 d_B' の組を生成し、データ格納部1004中にある元の表現 d_A 1007と d_B 1008を、新しい表現 d_A' と d_B' で書き換えるプログラムとなる。

表現変換プログラム1010を実行することにより、秘密鍵部分情報 d_A 1007と秘密鍵部分情報 d_B 1008の値が別の値に書き換わるため、データ格納部1004からバス1003を介して演算処理部1002へ流れるデータ、楕円曲線暗号復号プログラム1011を演算処理部1002で実行した時の時間、発生する電磁波の強さや消費電流等が異なったものとなる。これにより、TA(Timing Attack), DPA(Differential Power Analysis), SPA(Simple Power Analysis)等による秘密鍵の値の推定をさらに困難にすることが可能となる。

表現変換プログラム1010は、楕円曲線暗号復号プログラム1011が実行される直前に毎回実行されてもよいし、楕円曲線暗号復号プログラム1011が実行された直後に毎回実行されてもよい。あるいは楕円曲線暗号復号プログラム1011が何回か実行される毎に実行されてもよい。あるいはまた楕円曲線暗号復号プログラム1011の実行とは無関係に、ランダムなタイミングで実行されてもよい。楕円曲線暗号復号プログラム1011に対するTA(Timing Attack)やDPA(Differential Power Analysis)への対策としては、表現変換プログラム1010の実行頻度が多いほうが望ましい。

次に各プログラムの動作の詳細を説明する。

第2図は、第1図における表現変換プログラム1010のフローを示す。

ステップ2001：はじめ

ステップ2002：0以上n未満の乱数kを生成する

ステップ2003：データ格納部1004から秘密鍵部分情報d_A1007および秘密鍵部分情報d_B1008を読み込む

5 ステップ2004：d_A' = d_A + k (mod n) および d_B' = d_B + k (mod n) を計算する

ステップ2005：d_A' および d_B' をそれぞれデータ格納部1004中の秘密鍵部分情報d_A1007および秘密鍵部分情報d_B1008が書かれていたところに書き込む

10 ステップ2006：おわり

第3図は、第1図における楕円曲線暗号復号プログラム1011のフローを示す。

ステップ3001：はじめ

ステップ3002：Q = 0(無限遠点)とする

15 ステップ3003：ICカード1001の外部から復号用点R1013を読み込む

ステップ3004：データ格納部1004から秘密鍵部分情報d_A1007および秘密鍵部分情報d_B1008を読み込む

ステップ3005：i = |n| とする(|n|はベースポイントPの位数nのビット長)

20 ステップ3006：(d_A1007の第iビット目, d_B1008の第iビット目) = (1, 0) ならステップ3008へ(ここで第iビット目とは、最下位ビットを第1ビット目とし、上位に向かうほど大きくなるように数えるものとする)

ステップ3007：(d_A1007の第iビット目, d_B1008の第iビット目) = (0, 1) ならステップ3010へ、そうでなければステップ3009へ(ここで第iビット

25 目とは、最下位ビットを第1ビット目とし、上位に向かうほど大きくなるように数えるものとする)

ステップ3008: $Q = Q + R$ としてステップ3010へ(ここで + は楕円曲線上の点の加算を示す)

ステップ3009: $Q = Q - R$ としてステップ3010へ(ここで - は楕円曲線上の点の減算を示す)

5 ステップ3010: $i = i - 1$ とする

ステップ3011: $i > 0$ なら $Q = 2Q$ としてステップ3006へ(ここで $2Q$ は楕円曲線上の点Qの2倍算を示す)

ステップ3012: Qのx座標xQを復号用共通鍵として出力する

ステップ3013: おわり

10 なお, 上記ステップ3009における楕円曲線上の点の加算, ステップ3010における楕円曲線上の点の減算, および, ステップ3012における楕円曲線上の点の2倍算の詳細については, 文献[IEEEP1363]に詳しく述べられている。

15 楕円曲線暗号復号プログラム1011の手順は, 秘密鍵dの表現, 秘密鍵部分情報 d_A1007 および秘密鍵部分情報 d_B1008 がそれぞれ $d_A = d$, $d_B = 0$ となっている時には, バイナリ法と呼ばれる楕円曲線上の点のスカラー倍 dR を求めるために広く使われている方法と同じ手順となる。また, 秘密鍵dの表現, 秘密鍵部分情報 d_A1007 および秘密鍵部分情報 d_B1008 が, (d_A1007の第iビット目, d_B1008の第iビット目) = (1, 0)または(0, 1)となるようなビットの組が最も少なくなる表現となっている時には, 楕円曲線上の点のスカラー倍 dR を高速に求める手法として知られている, 最適な addition-subtraction chain を使った楕円曲線上の点のスカラー倍演算方法による演算, と同じ手順となる。

20 このように, 秘密鍵dの複数の表現方法を使い分けることは, 楕円曲線上の点のスカラー倍演算 dR を求める演算方法として, 知られている様々な演算方法を使い分けて演算することを意味している。結果的に,

この橜円曲線暗号復号プログラム1011の実行時間や発生する電磁波の強さや消費電流等はその表現方法毎に異なることになる。平均的には、バイナリ法を使った場合と同程度の処理時間となることが期待される。

addition-subtraction chainを使った橜円曲線上の演算方法について

5 は、

- 文献[ADD-SUB] F. Morain and J. Olivas "Speeding up the computations on an elliptic curve using addition-subtraction chains" Theoretical Informatics and Applications vol. 24, no. 6, 1990
に述べられている。

10 本実施例においては秘密鍵、それ自身を適当な機会に異なる表現方法によって保持し直すことにより、ICカード内には前記秘密にすべき情報そのものや、それに関する情報の固定された値は存在しないことになる。したがって例えば、攻撃者がデータ格納部1004に保存されたデータが演算処理部1002へうけわたされる時に情報が流れるバス1003の部分を解析
15 できたとしても、流れる情報から秘密にすべき情報を推定することは困難になる。

さらに、もし何らかの手段によって、データ格納部1004に保存されたデータの一部が攻撃者によって解析されたとしても、必ずしも、秘密にすべき情報をもらしたことにはならない。すなわち、秘密にすべき情報
20 それ自身が固定された値としてデータ格納部1004に保存されている場合には、その値の1ビットの情報が漏れたというのは秘密にすべき情報に関する情報の一部が漏れたことにはほかならないが、本発明にしたがって、秘密にすべき情報それ自身ではなく、それを表すある表現によって保持しておく場合には、たとえ、秘密にすべき情報dの表現であって、実際に
25 データ格納部1004に保存されているデータであるd_aとd_bの組のうち、その半分にあたるd_aの値が完全に漏れたとしても、秘密にすべき情報dその

ものに関しては、情報を漏らしていないことになる。

なぜなら、 d をどのような部分情報で、どのように表現しているかということを知らないからであるし、たとえ d_A と d_B の組で d を表していることを知っているとしても、 d_B の値や d_A と d_B の組でどのように d を表すかを知らないものにとっては、 d と d_A との間には何の関係も見出すことができないからである。
5

加えて、本発明では秘密にすべき情報を適切な時期に異なる表現方法によって保持し直しているので、攻撃者が後に、別の時点における d_B の値を知ったとしても、互いに異なる時点における d_A と d_B との間にはやはり何の関係も見出すことができないので、 d に関する情報は漏れることは10ない。

第4図は、第1図における共通鍵暗号復号プログラム1012のフローを示す。

ステップ4001：はじめ

15 ステップ4002：復号用共通鍵 c および暗号化されたメッセージ $m1014$ を入力する。ここで復号用共通鍵 c とは、楕円曲線暗号プログラム1011のステップ3011で出力された復号用共通鍵 xQ のことである

ステップ4003：復号用共通鍵 c と、暗号化されたメッセージ $m1014$ のビット長 L を、'key derivation function'への入力とし、出力として、長さ20 L のマスク列 M を得る。ここで、'key derivation function'とは、復号用共通鍵 c と出力されるマスク列の長さ L を入力として指定すると、長さ L のマスク列を出力するような関数であり、共通鍵暗号復号プログラム1012の一部として実装されているものとする。'key derivation function'の詳細については、文献[X9.63]に述べられている

25 ステップ4004：暗号化されたメッセージ $m1014$ とマスク列 M の排他的論理和 ($m' \text{ XOR } M$) を計算し、結果を復号化されたメッセージ $m'1015$ として

ICカード1001の外部に出力する

ステップ4005：おわり

本実施例においては、楕円曲線暗号の一種である Elliptic Curve Encryption Scheme (ECES) の復号化機能を持ったICカードに適用した例 5 を示したが、本発明は、これ以外にも広く適用可能である。

例えば、Elliptic Curve Encryption Scheme (ECES) ではなく、Elliptic Curve Augmented Encryption Scheme (ECAES) の復号化機能を持ったICカードに適用してもよい。この場合、本実施例の処理に加えて、あらかじめ暗号化されたデータと共に送られてきたMACと呼ばれるメッセージ検証用のデータを使って、復号されたデータが正しいものであるかどうかを検証する処理が加わる。Elliptic Curve Augmented Encryption Scheme (ECAES) についての詳細は、文献[X9.63]に述べられている。

あるいはまた、本実施例では、素数位数の有限体上の楕円曲線を利用していたが、標数2の有限体上の楕円曲線であってもよい。あるいはこれ以外の任意の有限体上の楕円曲線であってもよい。また、本実施例では、式 $y^2 = x^3 + a x + b$ で定義された楕円曲線を利用していたが、これ以外の式、例えば $b y^2 = x^3 + a x^2 + b x$ で定義された楕円曲線を利用してもよい。また、本実施例では、楕円曲線上の有理点が生成する群の上の、離散対数問題の困難性を利用した暗号を使っていたが、これ以外の群、例えば、有限体の乗法群、超楕円曲線上の因子類群、Cab曲線上の因子類群などの群の上の離散対数問題の困難性を利用した暗号であってもよい。これらの暗号を利用する場合には、上記の楕円曲線暗号復号プログラム1011中の楕円曲線上の点の秘密情報に基づく演算を、それぞれの群での秘密情報に基づく演算に置きかえればよい。

さらには、これら離散対数問題の困難性を利用した暗号以外の暗号であっても、より一般的には、暗号以外であっても、ある秘密にすべき数

5 あって、群演算をその秘密にすべき数だけ繰り返し行うような演算を含む機能を持ったICカードに対しても本発明は本実施例と同様にして適用可能である。すなわち、上記の楕円曲線暗号復号プログラム1011では、
Rを足すという演算を秘密にすべき数(秘密鍵d)回だけ行った結果である
10 dRを求めていたが、これと同様にして秘密にすべき数をある表現によつて表しておき、楕円曲線暗号復号プログラム1011に相当するプログラムによって、演算を行えばよい。このような暗号の例としては、上記の離散対数問題の困難性を利用した暗号以外に、例えば、RSA暗号などがある。
暗号以外の機能の例としては、RSA署名などがある。なお、ここで、群とは、集合であつて、その集合に属する各元の間にある演算が定義されて
いるようなもののことである。

RSA暗号・署名については、

* 文献[APPLIED] Bruce Schneier, "Applied Cryptography", John Wiley & Sons, Inc, 1996

15 に開示されている。

本実施例では、ICカードに適用した例を示したが、秘密にすべき情報より安全に保存する技術としてICカード以外にも広く適用可能である。例えば同じ機能を持つ、ICカード以外の secure cryptographic device や、半導体チップや、PCやワークステーションに対しても適用可能である。

・第2の実施例

第1の実施例において、楕円曲線暗号復号プログラム1011を次のように変形してもよい。

25 第5図は、本実施例におけるICカードの構成図である。この実施例においては、第1の実施例における楕円曲線暗号復号プログラム1011に該

当するプログラムは、次の2つのプログラム、テーブルデータ計算プログラム5001、テーブル参照型楕円曲線暗号復号プログラム5002からなる。

以下、各プログラムの動作の概略を説明する。

テーブルデータ計算プログラム5001は、ICカード1001の外部から与え
5 られる復号用点R1013を入力とし、テーブル参照型楕円曲線暗号復号プログラム5002で利用されるテーブルのデータを計算し、その結果をデータ格納部1004内のテーブルデータ5003領域に書き込むプログラムである。このプログラムは、データ格納部1004に含まれる秘密鍵dを表すデータ、すなわち本実施例における秘密鍵部分情報 d_A 1007と秘密鍵部分情報 d_B 1008、
10 には依存しない処理をおこなう。したがって、このプログラムが
TA(Timing Attack), DPA(Differential Power Analysis), SPA(Simple Power Analysis)などにより攻撃されても秘密鍵dに関するデータが漏れる心配はない。

テーブル参照型楕円曲線暗号復号プログラム5002は、データ格納部
15 1004に保存されている秘密鍵部分情報 d_A 1007および秘密鍵部分情報 d_B 1008と、テーブルデータ計算プログラム5001によって計算されたテーブルデータ5003から、暗号化されたメッセージm1014を共通鍵暗号復号プログラム1012で復号するために必要となる復号用共通鍵を計算するプログラムである。

20 次に各プログラムの動作の詳細を説明する。

第6図は、第5図におけるテーブルデータ計算プログラム5001のフローを示す。

ステップ6001：はじめ

ステップ6002：ICカード1001の外部から復号用点R1013を読み込む

25 ステップ6003：楕円曲線上の点 3R, 2R, R, -R, -2R, -3R を計算する

ステップ6004：テーブルデータ5003を、

$T[00][00] = 0$ (無限遠点),

$T[00][01] = -R$,

$T[00][10] = -2R$,

$T[00][11] = -3R$,

5 $T[01][00] = R$,

$T[01][01] = 0$ (無限遠点),

$T[01][10] = -R$,

$T[01][11] = -2R$,

$T[10][00] = 2R$,

10 $T[10][01] = R$,

$T[10][10] = 0$ (無限遠点),

$T[10][11] = -R$,

$T[11][00] = 3R$,

$T[11][01] = 2R$,

15 $T[11][10] = R$,

$T[11][11] = 0$ (無限遠点),

とし、データ格納部に保存する

ステップ6005：おわり

第7図は、第5図におけるテーブル参照型橜円曲線暗号復号プログラ
ム5002のフローを示す。

ステップ7001：はじめ

ステップ7002： $Q = 0$ (無限遠点)とする

ステップ7003：ICカード1001の外部から復号用点R1013を読み込む

ステップ7004：データ格納部1004から秘密鍵部分情報 d_A 1007および秘密
鍵部分情報 d_B 1008を読み込む

ステップ7005： $|n|$ が偶数なら $i = |n|$, $|n|$ が奇数なら $i = |n|+1$ とす

る($|n|$ はベースポイントPの位数nのビット長)

ステップ7006：データ格納部1004中のテーブルデータ5003を参照し， $S = T[d_A1007の第iビット目, d_A1007の第(i-1)ビット目][d_B1008の第iビット目, d_B1008の第(i-1)ビット目]$ とする(ここで第iビット目とは，最下位ビットを第1ビット目とし，上位に向かうほど大きくなるように数えるものとする)

ステップ7007： $Q = Q + S$ を計算する(ここで + は楕円曲線上の点の加算を示す)

ステップ7008： $i = i - 2$ とする

ステップ7009： $i > 0$ なら $Q = 4Q$ としてステップ7006へ(ここで $4Q$ は楕円曲線上の点Qの2倍算を2回繰り返すことによって求めることができる)

ステップ7010：Qのx座標xQを復号用共通鍵として出力する

ステップ7011：おわり

なお，上記ステップ7007における楕円曲線上の点の加算，および，ステップ7009における楕円曲線上の点の2倍算の詳細については，文献[IEEEP1363]に詳しく述べられている。

本実施例においては，秘密鍵部分情報の連続する2ビットずつに対して演算を行ったが，これとは異なるやり方でもよい。例えば，連続する3ビットずつに対して演算を行ってもよいし，一般に連続するtビットずつを対象としてよい。あるいは，互いにjビットはなれた($|n|/j$)個のビットを対象としてもよい。なおテーブルデータ計算プログラム5001はこれらの秘密鍵部分情報のビットの見方に応じて適切な値を計算するプログラムに変更する必要がある。

本実施例においても， dR を求める演算中に， d 自身の値は現れない。これにより dR を求める演算にかかる時間や発生する電磁波の強さや消

費電流は d そのものの値には依存しなくなる。したがってTA(Timing Attack), DPA(Differential Power Analysis)などにより攻撃によって、秘密鍵 d の値を推定することが困難になる。

本実施例においては、楕円曲線暗号の一種である Elliptic Curve

5 Encryption Scheme (ECES) の復号化機能を持ったICカードに適用した例を示したが、本発明は、第1の実施例と同様、これ以外にも広く適用可能である。特に、あるあらかじめ決まった元に対する群演算を秘密にすべき数だけ繰り返し行うような演算を含む処理を行う装置に適用する場合には、テーブルデータ計算プログラム5001を毎回実行する必要はなく、
10 一度だけ実行すればよいため、毎回の処理が高速に実行可能となり一層有効である。この場合には、さらに、テーブルデータの計算を装置(本実施例の場合で言えばICカード1001)の外部で行うことも可能である。このような処理を含む装置の例としては、例えば、楕円曲線暗号における鍵生成処理を行うICカードが挙げられる。この場合、乱数として生成した
15 秘密鍵情報 d と、固定点であるベースポイント P から楕円曲線上の点 dP を求める処理が含まれる。したがって、テーブルデータは、例えば、ICカードの外部で計算しておき、システム鍵情報の一部としてICカード内にあらかじめ保存しておくことが可能である。

20 · 第3の実施例

第2の実施例において、テーブルデータ5003領域へのテーブルデータの保存方法を次のようにしてもよい。

25 楕円曲線上の点は通常2次元affine座標を用いて、 x 座標および y 座標の2つの値の組によって表現されるが、点の加算や点の2倍算を行う場合に、主として高速に演算を行う目的で、 x 座標、 y 座標および z 座標の3つの値の組によって表現することも可能である。このような表現および

この表現を使った場合の橿円曲線上の点の演算方法の一例が文献

[IEEEP1363]に projective coordinate として述べられている。2次元 affine座標による表現と projective coordinate による表現との間の相互変換は次のように行うことができる。

5 [2次元affine座標から projective coordinate へ] $(x, y) \rightarrow [x, y, 1]$
 [projective coordinate から2次元affine座標へ] $[X, Y, Z] \rightarrow (X/Z^2, Y/Z^3)$

ここで注意すべき事は、 projective coordinate による表現では、同じ点を表す表現は一通りではないということである。すなわち、 t を $0 < t < p$ (p は橿円曲線の定義される有限体の位数) となる数とすると、点 $[X, Y, Z]$ と点 $[t^2 X, t^3 Y, t Z]$ は、共に同じ点 $(X/Z^2, Y/Z^3)$ を表している。

第2の実施例におけるテーブルデータ5003領域へのテーブルデータの保存方法として、この projective coordinate による表現で保存しておくことができる。この場合、同じ点を表すデータであっても、異なる表現によって保存しておくことが可能となる。例えば $T[10][00]$ と $T[11][01]$ は共に点2Rを表すデータが保存されているが、これら2つをそれぞれ異なる表現、すなわち、 $T[10][00]=[X, Y, Z]$, $T[11][01]=[X', Y', Z']$ (ここで $X/Z^2 = X'/Z'^2$, $Y/Z^3 = Y'/Z'^3$ を満たすものとする) を使って保存しておくことにより、テーブル参照型橿円曲線暗号復号プログラム5002の実行中に $T[10][00]$ が参照された場合と $T[11][01]$ が参照された場合とで、演算処理が異なることになり、その結果、実行にかかる時間、発生する電磁波の強さおよび消費電流等も異なることになる。

第8図は、本実施例におけるICカードの構成図である。本実施例では、
 25 第2の実施例に点表現変換プログラム8001が追加されている。

以下、点表現変換プログラム8001の概略を説明する。

点表現変換プログラム8001はデータ格納部1004に保存されているテーブルデータ5003中の点の表現を変換し、変換した値によってテーブルデータ5003を書き換える。なお、テーブルデータ5003は、テーブルデータ計算プログラム5001によって、projective coordinate で表されたx座標、y座標およびz座標の3つの値の組によって表現され保存されているものとする。すなわち、例えば、2次元affine座標によって(x, y)と表現されているものを[x, y, 1]に変換して保存してもよいし、あるいは、テーブルデータ計算プログラム5001のステップ6003でテーブルデータ5003を計算する際に、projective coordinate を使って計算を行い、その結果をprojective coordinate のままテーブルデータ5003に保存してもよい。点表現変換プログラム8001はテーブルデータ計算プログラム5001の実行後から、最後にテーブルデータ5003が参照されるまでの間の任意の時点に実行されてよい。また、この間に何度実行されてもよい。例えば、テーブル参照型楕円曲線暗号復号プログラム5002が実行される直前に実行されてもよいし、あるいは、テーブルが参照される機会が一度でもものこっているのならテーブル参照型楕円曲線暗号復号プログラム5002の実行中に割り込む形で実行されてもよい。

次に、点表現変換プログラム8001の詳細を説明する。

第9図は、第8図における点表現変換プログラム8001のフローを示す。

20 ステップ9001：はじめ

ステップ9002：i = 00 とする

ステップ9003：j = 00 とする

ステップ9004：[x, y, z] = T[i][j] を読み込む

25 ステップ9005：乱数kを生成する(0 < k < p とする。p は楕円曲線の定義される有限体の位数)

ステップ9006：[x, y, z] = [k² x (mod p), k³ y (mod p), k z (mod p)]

とする(p は橜円曲線の定義される有限体の位数)

ステップ9007: $T[i][j] = [x, y, z]$ とする

ステップ9008: $j = j + 1$ とする(ただし j は2進法で表記されているとする)

5 ステップ9009: $j \leq 11$ (2進法表記)ならステップ9005へ

ステップ9010: $j = 00$ とする

ステップ9011: $i = i + 1$ とする(ただし i は2進法で表記されているとする)

ステップ9012: $i \leq 11$ (2進法表記)ならステップ9005へ

10 ステップ9013: おわり

本実施例においては、適当なタイミングで点表現変換プログラム8001を実行することにより、同じ点を表す複数のデータ、例えば $T[10][00]$ と $T[11][01]$ は、異なる表現によって保存されることになり、また、同じデータ $T[i][j]$ であっても、それを参照するタイミングによって異なる表現になっているため、テーブルデータ5003を参照する演算を含む処理は、たとえ入力が毎回同じであっても、異なるものとなる。したがって、処理時間や発生する電磁波の強さや処理中の消費電流等も一定ではない。これはすなわち、秘密鍵とテーブルデータ5003を使った演算、テーブル参照型橜円曲線暗号復号プログラム5002の実行にかかる時間や発生する電磁波の強さや、消費電流が一定ではないことを意味する。したがってTA(Timing Attack), DPA(Differential Power Analysis)などの攻撃によって、秘密鍵の値を推定することが困難になる。

本実施例においては、点表現変換プログラム8001によって、テーブルデータ5003に含まれるすべての点情報の変換を行ったが、すべての点ではなく、ランダムに選んだ1つまたは複数の点のデータだけを変換してもよい。テーブル参照型橜円曲線暗号復号プログラム5002に対する

TA(Timing Attack)やDPA(Differential Power Analysis)への対策としては、多くの点データの表現を変換したほうが望ましく、また、点表現変換プログラム8001の実行頻度が多いほうが望ましい。

本実施例においては、楕円曲線暗号の一種である Elliptic Curve Encryption Scheme (ECES) の復号化機能を持ったICカードに適用した例を示したが、本発明は、第2の実施例と同様、これ以外にも広く適用可能である。

・第4の実施例

第1の実施例において、秘密にすべき情報、すなわち秘密鍵dは、秘密鍵部分情報 d_A1007 と秘密鍵部分情報 d_B1008 の組によって表現されていた。より具体的には、 d_A1007 と d_B1008 の法nにおける差が秘密鍵dの値と等しくなるように表現されていた。また、第1の実施例においては、 d_A1007 と d_B1008 は、0以上n未満の数として表現されていた。しかしながらこれ以外の方法で表現されていてもよい。例えば d_A1007 は、0以上2n未満の数として表現されていてもよい。あるいは、和や差が秘密鍵dの値と等しくなるような3つ以上の数の組として表現されていてもよい。

あるいは、別の表現として、例えば、次のように、1, 0, -1の並びとしてdの値が表現されていてもよい。すなわち表現 $(B_n, B_{n-1}, \dots, B_1, B_0)$ は、数 $2^n B_n + 2^{n-1} B_{n-1} + \dots + 2^1 B_1 + 2^0 B_0$ を表すものとする。ここで、 B_i は、1, 0, -1のいずれかであるとする。この表現は通常の2進表現の拡張になっている。すなわち、この表現方法で、 B_i を0か1のどちらかだけであるように制限したものが通常の2進表現である。なお、1, 0, -1をメモリ上で表現するためには、2ビット分を使って、00なら0, 01なら1, 11なら-1を表す、といった方法が考えられる。

この表現を使った時には、第1の実施例における表現変換プログラム

1010は、例えば、次のように変更される。なお、データ格納部1004には、
秘密鍵部分情報d_a1007と秘密鍵部分情報d_b1008の組の代わりに、1, 0, -1
の並びとして表現された秘密鍵情報d_{rep}が保存されているものとする。
表現変換プログラム(拡張2進表現)

5 ステップ10001：はじめ

ステップ10002：データ格納部1004から秘密鍵情報d_{rep}を読み込む

ステップ10003：乱数K, Lを生成する(ここで $0 < K < L < |d_{rep}|$ とする。
ただし $|d_{rep}|$ はd_{rep}のビット長)

ステップ10004：秘密鍵情報d_{rep}の第L+1ビット目の値B_{L+1}を $B_{L+1} = B_{L+1} +$

10 1 とする

ステップ10005： $K < i \leq L$ なるすべての i に対し、秘密鍵情報d_{rep}
の第iビット目の値B_iを $B_i = B_{i-1}$ とする

ステップ10006：秘密鍵情報d_{rep}の第Kビット目の値B_Kを $B_K = B_K - 2$ と
する

15 ステップ10007：秘密鍵情報d_{rep}の各ビットが 1, 0, -1 のいずれかであ
ればステップ10013へ

ステップ10008： $j = |d_{rep}|$ とする

ステップ10009：d_{rep}の第jビット目の値B_jが2であったら $B_{j+1} = B_{j+1} + 1$,
 $B_j = 0$ とする

20 ステップ10010：d_{rep}の第jビット目の値B_jが-2であったら $B_{j+1} = B_{j+1} -$
1, $B_j = 0$ とする

ステップ10011： $j = j - 1$ とする

ステップ10012： $j > 0$ ならステップ10007へ

ステップ10013：データ格納部1004に更新された秘密鍵情報d_{rep}を書き
25 込む

ステップ10014：おわり

また、第1の実施例における楕円曲線暗号復号プログラム1011は、次のように変更される。

楕円曲線暗号復号プログラム(拡張2進表現)

[ステップ3004]を次のように変更

5 ステップ11004：データ格納部1004から秘密鍵情報d_repを読み込む

[ステップ3006]を次のように変更

ステップ11006：d_rep1の第iビット目B_iが1ならステップ3009へ

[ステップ3007]を次のように変更

ステップ11007：d_rep1の第iビット目B_iが-1ならステップ3010へ

10 本実施例では、1, 0, -1の並びとしてdの値が表現されていたが、同様に2進表現の拡張を使って、例えば、2, 1, 0, -1の並びとしてdの値を表現してもよい。また、t, t-1, , 0, -1, , -s (s, t ≥ 0)の並びとしてdの値を表現してもよい。さらには、あらゆるdの値を表現できるのであれば、必ずしも連続していないいくつかの数の並びとしてdの値を表現してもよい。

あるいはまた、秘密鍵情報dの値の別の表現として、積がdと等しくなるような2つの数の組として表現されていてもよい。すなわち、第1の実施例における秘密鍵部分情報d_A1007と秘密鍵部分情報d_B1008の組の代わりに、d_{m_A} × d_{m_B} (mod n) が秘密鍵情報dの値と等しくなるような2つの数の組d_{m_A}とd_{m_B}がデータ格納部1004に保存されているようにしてもよい。あるいは、積がdと等しくなるような3つ以上の数の組によって表現されていてもよい。さらには、積とは限らず、あらかじめ決められた演算結果が秘密鍵情報dとなるような複数の数の組によって表現されていてもよい。なお、これら様々な秘密情報生成情報による表現方法を用いる場合には、それらを正しく処理できる秘密情報生成情報処理手段を併せて用いることで所望の結果を得られる。

積がdと等しくなるような2つの数の組による表現を使った時には、第1の実施例における表現変換プログラム1010は、例えば、次のように変更される。

表現変換プログラム(積表現)

5 ステップ12001：はじめ

ステップ12002：0より大きくn未満の乱数kを生成する

ステップ12003：データ格納部1004から d_{m_A} および d_{m_B} を読み込む

ステップ12004： $d_{m_A}' = k \cdot d_{m_A} \pmod{n}$ および $d_{m_B}' = k^{-1} \cdot d_{m_B} \pmod{n}$ を計算する

10 ステップ12005： d_{m_A}' および d_{m_B}' をそれぞれデータ格納部1004中の d_{m_A} および d_{m_B} が書かれていたところに書き込む

ステップ12006：おわり

また、第1の実施例における楕円曲線暗号復号プログラム1011は、次のように変更される。

15 楕円曲線暗号復号プログラム(積表現)(概略)

ステップ13001：はじめ

ステップ13002：ICカード1001の外部から復号用点R1013を読み込む

ステップ13003：データ格納部1004から d_{m_A} および d_{m_B} を読み込む

ステップ13004： $Q = d_{m_A} \cdot R$ を計算する

20 ステップ13005： $Q = d_{m_B} \cdot Q$ を計算する

ステップ13006： Q のx座標xQを復号用共通鍵として出力する

ステップ13007：おわり

なお、上記ステップ13004および13005における楕円曲線上の点のスカラーバイ倍演算は、任意の方法で行ってよい。例えば、バイナリ法を使って

25 演算してもよいし、あるいは、 d_{m_A} や d_{m_B} を秘密鍵の値そのものと見なして他の実施例に示した方法を利用して演算してもよい。

以上、秘密情報を表す表現方法の例をいくつか示したが、これらを組み合わせてもよい。例えば、異なる、あるいは、同じ表現方法による複数の表現をデータ格納部1004に持っておき、実際に秘密情報を利用する演算を行う時に、これらのうちのひとつまたは複数をランダムに選び演算をおこなってもよい。また、これらの表現を処理する複数の処理手段を持っておき、実際に秘密情報を利用する演算を行う時に、これらのうちのひとつまたは複数をランダムに選び演算をおこなってもよい。

あるいは、秘密分散と呼ばれる手法により、あらかじめ秘密情報を n 個中の k 個がそろった時に元の情報が復元できるような n 個に分散しておき、これら n 個の情報を秘密情報の表現としてもよい。

秘密分散については、

文献[Shamir] Adi Shamir, "How to Share a Secret", Communications of the ACM vol. 22, no. 11, pp. 612-613, 1979
に開示されている。

これらの手段により、秘密裏に保存すべき情報を利用する演算を行った時に要する時間や発生する電磁波の強さや消費電流を一定ではないようになることが可能となり、TA(Timing Attack), DPA(Differential Power Analysis), SPA(Simple Power Analysis)等によって秘密鍵の値を推定することが困難になる。

本実施例においては、楕円曲線暗号の一種である Elliptic Curve Encryption Scheme (ECES) の復号化機能を持ったICカードに適用した例を示したが、本発明は、第1の実施例と同様、これ以外にも広く適用可能である。

25 · 第5の実施例

第1から第4までの実施例においては、主として、本発明を、秘密鍵 d

と与えられた楕円曲線上の点Rに対し, dR を計算する処理に適用した例を示したが, 本発明は, これ以外の処理に対しても有効である。

本発明を, 楕円曲線を利用したディジタル署名方式である ECDSA 署名の署名生成機能を持ったICカードに適用した一実施例を, 以下, 図を用いて説明する。 ECDSA署名については, 前記文献[IEEEP1363]の他, 文献[X9. 62] "Working Draft AMERICAN NATIONAL STANDARD X9. 62-1998 Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)", American National Standards Institute, September 20, 1998 に開示されている。

なお, 本実施例において, 秘密裏に保存すべき情報に該当する情報は, ECDSA署名の生成に必要とされる秘密鍵である。また本実施例では, 素数位数の有限体上の楕円曲線を利用するものとする。

第10図は, 本実施例におけるICカードの構成図である。第1の実施例におけるICカードの構成図である第1図との相違点は, 第10図には楕円曲線暗号復号プログラム1011と共に鍵暗号復号プログラム1012がないこと, 第10図にはECDSA署名生成プログラム14001があること, ICカード1001に対する入出力が異なること, および, 第10図では秘密鍵部分情報 d_A1007 と秘密鍵部分情報 d_B1008 の組が表す情報が楕円曲線暗号復号用秘密鍵ではなくECDSA署名生成用秘密鍵を意味すること, である。第1図と共に要素については同じ番号が振ってある。

ECDSA署名生成プログラム14001について説明する。

ECDSA署名生成プログラム14001は, ICカード1001の外部から署名対象メッセージ14002を入力し, また, データ格納部1004から秘密鍵部分情報 d_A1007 および秘密鍵部分情報 d_B1008 を入力し, デジタル署名14003を計算し, ICカード1001の外部に出力する。電子的な署名対象メッセージに

対するデジタル署名は、紙の書類に対する印影に相当するもので、署名対象メッセージの内容を、署名者すなわち秘密鍵の所有者が保証したことを見出す証拠になる。ECDSA署名の詳細については、文献[X9.62]に詳しく述べられている。

5 ICカード1001を使った時の署名対象メッセージ14002に対する署名生成を行う時の表現変換プログラム1011およびECDSA署名生成プログラム14001による基本的な動作の流れをまとめると次のようになる。

まず、ECDSA署名生成プログラム14001が、ICカード1001の外部からの入力である署名対象メッセージ14002と、データ格納部1004に保存された秘密鍵部分情報 d_A 1007と秘密鍵部分情報 d_B 1008から、秘密鍵 d を求めることなくデジタル署名14003を計算し、ICカード1001の外部に出力する。これにより、デジタル署名を生成することができる。

10 このように秘密鍵 d がデータ格納部1004、バス1003、演算処理部1002に出現することなくデジタル署名14003を生成することができるので、TA(Timing Attack), DPA(Differential Power Analysis), SPA(Simple Power Analysis)等によって秘密鍵の値を推定することが困難になっている。

この例では、データ格納部1004に保存された秘密鍵部分情報 d_A 1007と秘密鍵部分情報 d_B 1008の値が固定されている。したがって、署名生成を行うたびに、固定値である秘密鍵部分情報 d_A 1007と秘密鍵部分情報 d_B 1008がデータ格納部1004からバス1003を介して演算処理部1002に毎回流れることになり、また、ECDSA署名生成プログラム14001は、毎回同じ値を使って計算を行うことになるため、この間の計算時間や発生する電磁波の強さや消費電流等もこの固定された値に依存する。このことはTA(Timing Attack), DPA(Differential Power Analysis), SPA(Simple Power Analysis)等によって秘密鍵部分情報の値を推定される可能性がある。

あることを意味する。

本発明では、これらの攻撃に対するさらなる対策として、第1の実施例と同様に、表現変換プログラム1010を利用する。すなわち、表現変換プログラム1010を実行することにより、秘密鍵部分情報 d_A 1007と秘密鍵部分情報 d_B 1008の値が別の値に書き換わるため、データ格納部1004からバス1003を介して演算処理部1002へ流れるデータ、ECDSA署名生成プログラム14001を演算処理部1002で実行した時の時間や発生する電磁波の強さや消費電流等も異なったものとなる。これにより、TA(Timing Attack)、DPA(Differential Power Analysis)、SPA(Simple Power Analysis)等による秘密鍵の値の推定をさらに困難にすることが可能となる。

表現変換プログラム1010は、ECDSA署名生成プログラム14001が実行される直前に毎回実行されてもよいし、ECDSA署名生成プログラム14001が実行された直後に毎回実行されてもよい。あるいはECDSA署名生成プログラム14001が何回か実行される毎に実行されてもよい。あるいはまたECDSA署名生成プログラム14001の実行とは無関係に、ランダムなタイミングに実行されてもよい。ECDSA署名生成プログラム14001に対するTA(Timing Attack)やDPA(Differential Power Analysis)への対策としては、表現変換プログラム1010の実行頻度が多いほうが望ましい。

次にECDSA署名生成プログラム14001の詳細について説明する。

第11図は、第10図におけるECDSA署名生成プログラム14001のフローを示す。

ステップ15001：はじめ

ステップ15002：ICカード1001の外部から署名対象メッセージ14002を読み込む

ステップ15003：署名対象メッセージ14002をハッシュ関数の入力としメッセージのハッシュ値 h を得る

ステップ15004: データ格納部1004から秘密鍵部分情報 d_A 1007および秘密鍵部分情報 d_B 1008を読み込む

ステップ15005: 乱数 k を生成する($0 < k < n$ とする)

ステップ15006: $(x, y) = k P$ を計算する

5 ステップ15007: $r = x \pmod n$ とする

ステップ15008: $s_A = k^{-1} (d_A r + h) \pmod n$ を計算する

ステップ15009: $s_B = k^{-1} (d_B r + h) \pmod n$ を計算する

ステップ15010: $s = s_A - s_B \pmod n$ を計算する

ステップ15011: (r, s) をデジタル署名として出力する

10 ステップ15012: おわり

ここで特徴的な事は、秘密鍵 d の値それ自身、すなわち、 $d_A - d_B \pmod n$ はこのECDSA署名生成プログラム14001中に一度も現れないが、結果として得られた s は、

$$s = s_A - s_B \pmod n$$

$$15 = k^{-1} (d_A r + h) - k^{-1} (d_B r + h) \pmod n$$

$$= k^{-1} (d r + h) \pmod n$$

を満たすため、秘密鍵 d をつかって計算したのと同じ結果が得られているということである。

20 このように、本実施例においても、 d_A と d_B にわけて保存していることを活かした処理を行うことで、上記実施例と同様の効果が得られる。なぜなら、せっかく秘密鍵を、秘密鍵部分情報に分けて保存しておいても、例えば、一旦 $d = d_A - d_B$ という計算によって求めた d の値を使って ECDSA 署名生成を行ってしまっては、効果が減少してしまうからである。

さらに、第1の実施例と同様に、表現変換プログラム1010によって、
25 秘密鍵 d の表現である秘密鍵部分情報 d_A 1007および秘密鍵部分情報 d_B 1008の組を変更することにより、ECDSA署名生成プログラム14001、よ

り詳しくは、ECDSA署名生成プログラム14001のステップ15008中の掛け算 $d_A \cdot r$ およびステップ15009中の掛け算 $d_B \cdot r$ の、実行にかかる時間や発生する電磁波の強さや消費電流は秘密鍵 d そのものの値には依存しなくなる。したがってTA(Timing Attack), DPA(Differential Power Analysis)など5により攻撃によって、秘密鍵の値を推定することがさらに困難になるという効果が得られる。

本実施例では、署名対象メッセージのメッセージダイジェストであるハッシュ値をICカード1001の内部で、ECDSA署名生成プログラム14001のステップ15003で求めたが、この処理はICカード1001と情報のやり取りができる外部の装置、例えば、ICカード1001とICカードリーダライタを通じて情報のやり取りができるPC等で行ってもよい。この場合、ICカードに対する入力は、署名対象メッセージのハッシュ値となる。

本実施例において、ECDSA署名生成プログラム14001のステップ15005で生成される乱数 k も秘密に保持すべき値である。なぜなら、デジタル署名 (r, s) 、秘密鍵 d 、乱数 k 、ハッシュ値 h らの間には、 $s = k^{-1} (d \cdot r + h) \pmod n$ という関係があり、これらのうち、 r, s, h は誰もが知ることができる値であるため、もし、乱数 k の値が分かれば、秘密鍵 d の値も計算によって分かってしまうからである。

ただし、秘密鍵 d の値が一定であるのに対し、乱数 k は署名を生成するたびごとにランダムに生成される点で異なるため、TA(Timing Attack), DPA(Differential Power Analysis)などの攻撃によって値が推定される可能性は秘密鍵に比べて低い。なお、ここで、秘密鍵 d の値が一定であるというのは、具体的な表現のことではなく、本来持っている情報の内容のことである。

25 なお、より安全性を高める目的で、乱数 k に対しても、本発明を適用することは可能である。例えば、第2の実施例と同様にして次のように行

うことができる。すなわち、まず、第2の実施例におけるテーブルデータ計算プログラム5001により、テーブルデータを計算しておく。本実施例においては、固定された点であるベースポイントPに関するテーブルなので、第2の実施例中の説明中で述べたように、テーブルデータは事前に、例えばICカード1001の外部で、計算しておくことが可能である。

ECDSA署名生成プログラム14001のステップ15005で乱数kを生成した後、これを k_A と k_B の組として表現してデータ格納部1004に保存し、さらに表現変換プログラムにより変換する。その後ECDSA署名生成プログラム14001のステップ15006における(x, y)を、第2の実施例におけるテーブル参照型橿円曲線暗号復号プログラム5002と同様にして計算する。ECDSA署名生成プログラム14001のステップ15008およびステップ15009で使う値 k^{-1} は、例えば、次のようにして計算すればよい。まず、 $t = k_B^{-1} - k_A^{-1} \pmod n$ を計算する。次に $t^{-1} k_A^{-1} k_B^{-1} \pmod n$ を計算する。これが k^{-1} と等しくなる。

ここで特徴的な事は、この k^{-1} を求める演算中に、k自身の値は現れないことである。これにより k^{-1} を求める演算にかかる時間や発生する電磁波の強さや消費電流はkそのものの値には依存しなくなる。したがってTA(Timing Attack), DPA(Differential Power Analysis)などにより攻撃によって、乱数kの値を推定することが困難になる。

本実施例においては、ディジタル署名の一種であるECDSA署名の署名生成機能を持ったICカードに適用した例を示したが、本発明は、これ以外にも広く適用可能である。

例えば、利用する橿円曲線は、第1の実施例で述べた他の橿円曲線でもよい。また、橿円曲線上の離散対数問題の困難性を利用したディジタル署名にかぎらず、第1の実施例で述べた他の群の上の離散対数問題の困難性を利用したディジタル署名であってもよい。

あるいは、ディジタル署名でなくても、より一般に、群G1から群G2への準同型写像 f があって、秘密裏に保持すべき群G1の元 g から群G2の元 $f(g)$ を計算する装置がある時、この装置に対するTA(Timing Attack), DPA(Differential Power Analysis), SPA(Simple Power Analysis)等により g が推定される可能性は、本発明によれば、例えば、次のようにして減らすことができる。

まず $g = g_1 \cdot g_2$ (・は群G1の演算を表す)となる g_1 と g_2 の組により g を表現し、データ保存部に保存しておく。

次に、ランダムに選んだG1の元 h について、 $g_1' = h \cdot g_1$, $g_2' = h^{-1} \cdot g_2$ (h^{-1} は群G1の演算・に関する h の逆元を表す)を計算し、 g_1 を g_1' で g_2 を g_2' でおきかえるプログラムを実行する。これを表現変換プログラムと呼ぶ。最後に、 $f(g)$ の値を得るために、 $f(g_1) \# f(g_2)$ (#は群G2の演算を表す)を計算する。 f は準同型写像だから、 $f(g_1) \# f(g_2)$ は $f(g)$ に等しい。

このように適宜、表現変換プログラムを実行するたびに、その後の $f(g)$ の値を求める処理に要する時間や発生する電磁波の強さや消費電流は異なるものになる。これにより、TA(Timing Attack), DPA(Differential Power Analysis), SPA(Simple Power Analysis)等によって秘密鍵の値を推定することが困難になる。なお、ここで、準同型写像とは、群から群への写像であって、演算を保つような写像のことである。

20

・第6の実施例

本発明を、電子商取引におけるメッセージの送受に適用した一実施例を、以下、図を用いて説明する。

以下の実施例では、一般消費者であるカードホルダが、販売店であるマーチャントに対し、商品の購入要求を行う時の処理について説明する。

図12は、本実施例におけるシステム構成図である。図12において、

ネットワーク16001に、一般消費者であるカードホルダのコンピュータ16002、販売店であるマーチャントのコンピュータ16003、および、認証局16004が接続されている。ここで、認証局とは、公開鍵の正当性を保証する証明書を発行する機関である。

5 カードホルダのコンピュータ16002は、CPU16005、メモリ16006からなり、ディスプレイ16007、キーボード16008、および、ICカードリーダライタ16009が接続されており、また、ネットワーク16001に接続されている。カードホルダはまた署名用ICカード16010を所有しており、署名用ICカード16010とコンピュータ16002とは、ICカードリーダライタ16009を通して、情報のやり取りが可能となっている。この署名用ICカード16010は、第5の実施例に示したICカードと同じものである。

マーチャントのコンピュータ16003は、CPU16011、メモリ16012からなり、ディスプレイ16013、および、キーボード16014が接続されており、また、ネットワーク16001に接続されている。

15 カードホルダのコンピュータ16002のメモリ16006内には公開鍵16015が、また、カードホルダの所有する署名用ICカード16010のメモリ内には、公開鍵16015とペアになる秘密鍵に係わる情報やプログラムが、本発明を適用した形で保存されている。これらの情報は、カード発行者、例えばクレジット会社、によって、あらかじめ秘密鍵に係わる情報やプログラムが書き込まれたICカードと、公開鍵情報が入ったFDやCD-ROMなどの記録媒体が、送られてくることにより設定されるものである。あるいは、公開鍵情報は有線無線などの伝送媒体によって送られてくるものとしてもよい。あるいは、カード発行者から送られてきたICカードに鍵生成機能が組み込まれていて、それをカードホルダが実行することによって設定されるものとしてもよい。あるいはまた、カード発行者から、カードホルダのコンピュータ上で実行可能な鍵生成プログラムが、FDやCD-ROM

などの記録媒体や有線無線などの伝送媒体によって送られてきて、それをカードホルダが実行することによって、送られてくるICカードに設定されるものとしてもよい。鍵生成機能付きのICカードを利用する方法の場合は、秘密鍵に関する情報が、ICカードの外部に漏れることがないため、セキュリティ上の観点からはこの方法が一番望ましい。なお、ICカード内の秘密鍵は、第5の実施例と同様に、本発明を適用した保存方法によって保存されているものとする。また、上記実施例を適用した秘密情報生成情報による秘密情報の表現方法やその秘密情報生成情報を処理するプログラムは、個々のICカードによって異ならせても良いし同じであっても良い。異なる方がより安全性が高まる。

マーチャントのコンピュータ16003のメモリ16012内には、あらかじめ、署名検証プログラム16018、および、システム鍵16019が設定されている。これらは、カードホルダの所有する署名用ICカード16010に対応するよう15に設定されているものとする。署名検証プログラム16018の詳細については、文献[X9.62]に述べられている。

次に、カードホルダの行う処理について説明する。

はじめにカードホルダは、認証局16004に公開鍵証明書16016を発行してもらうため、公開鍵16015を送る。認証局16004はカードホルダからの要求に応じ、周知の方法で、公開鍵証明書16016を発行してカードホルダのコンピュータ16002に送る。この処理は一つの公開鍵に対し一度だけ必要な処理である。言い換えると、購入要求メッセージを送信する処理を行なうたびに必要なわけではない。また、認証局が公開鍵証明書を発行する手順中には、デジタル署名を生成する過程が含まれるため、この過程に対しても本発明を適用することは可能である。

次に、カードホルダが購入要求メッセージをマーチャントに送信する際の処理について、説明する。

カードホルダのコンピュータ16002は、購入要求メッセージ16017を作成し、メモリ16006内に保存する。この購入要求メッセージ16017をICカードリーダライタ16009を通じて、署名用ICカード16010に送り、本発明による方法に従ってディジタル署名16020を生成させ、これもメモリ16006
5 内に保存する。

このディジタル署名16020が、購入要求メッセージ16017の内容が確かにカードホルダによって確認されたことを示す証拠となり、通常の紙の書類における印影に相当する。すなわち、通常の紙の書類に対する印鑑に相当するのが、署名用ICカード16010内に保存された秘密鍵になる。し
10 たがって、もし、署名用ICカード16010内に保存された秘密鍵を、悪意のある人が知ってしまうと、正当な所有者であるカードホルダになりすまして、購入要求を行うことができるようになってしまう。

本実施例によれば、今まで述べてきたように署名用ICカードに対するこれらの攻撃法により秘密鍵を推定することが困難になる。

15 カードホルダのコンピュータ16002は、ディジタル署名16020を生成した後、購入要求メッセージ16017、公開鍵16015、公開鍵証明書16016、および、ディジタル署名16020をまとめて送信文16021として、ネットワーク16001を通じて、マーチャントに送る。

マーチャントは、送信文16021を受け取ると、まず、周知の方法により、
20 公開鍵証明書16016を使って公開鍵16015が正当なものであることを確認した後、署名検証プログラム16018を実行することにより、購入要求メッセージ16017が確かにカードホルダによって作成されたものかどうかを、
25 ディジタル署名16020、公開鍵16015およびシステム鍵16019などを利用して調べる。その結果、ディジタル署名16020の正当性が確認されれば、
購入要求メッセージ16017の内容は信頼できるものであるとし、取引を継続する。一方、もしディジタル署名16020の正当性が確認されなければ、

ネットワーク16001中で改ざんされた、あるいは、正しいカードホルダでない人によって購入要求メッセージ16017が作成された等、何らかの不正があったものとし、取引は中止する。

5 産業上の利用可能性

本発明により、各種攻撃法に対して安全な、演算方法および情報の保持方法およびこれらの方法を利用したICカード、セキュリティモジュール、半導体チップ、システム、コンピュータ、プログラムを提供することができる。

請求の範囲

1.

演算処理回路と記憶回路とそれらを接続する信号線とで構成した秘密情報の処理装置において、

5 秘密情報と処理対象となるデータとを既知の処理方法に基づいて処理した処理結果と同一の処理結果を得るように構成された秘密情報の処理装置であって、

前記記憶回路は、

前記秘密情報とは異なる秘密情報生成情報と、

10 前記秘密情報生成情報と前記処理対象となるデータとを用い、前記秘密情報を前記演算処理回路や前記記憶回路や前記信号線に出現させることなく、前記処理結果を出力する秘密情報生成情報処理手段とを保持し、前記演算処理回路は、前記秘密情報生成情報処理手段を実行することを特徴とする秘密情報の処理装置。

15

2.

請求項 1 記載の秘密情報の処理装置において、

前記記憶回路は、前記秘密情報生成情報を複数の秘密情報部分情報として保持することを特徴とする秘密情報の処理装置。

20

3.

請求項 1 または 2 記載の秘密情報の処理装置において、

前記記憶回路は、前記秘密情報生成情報を他の秘密情報生成情報へ変換する変換手段をさらに備え、

25 前記他の秘密情報生成情報は、前記秘密情報生成情報処理手段が前記処理結果と同一の処理結果を出力させる情報であることを特徴とする秘

密情報の処理装置。

4.

請求項 1ないし 3いずれか一に記載の秘密情報の処理装置において、

5 前記秘密情報は、公開鍵暗号技術における、復号化またはディジタル署名を生成するための秘密鍵であることを特徴とする秘密情報の処理装置。

5.

10 請求項 1ないし 4いずれか一に記載の秘密情報の処理装置において、前記演算処理回路は、前記変換手段を、所定の時期に実行することを特徴とする秘密情報の処理装置。

6.

15 演算処理回路と記憶回路とそれらを接続する信号線とで構成した処理装置における秘密情報の処理プログラムにおいて、
秘密情報と処理対象となるデータとを既知の処理方法に基づいて処理した処理結果と同一の処理結果を得るように構成された秘密情報の処理プログラムであって、

20 前記秘密情報とは異なる秘密情報生成情報と前記処理対象となるデータとを用い、

前記秘密情報を前記演算処理回路や前記記憶回路や前記信号線に出現させることなく、

前記演算処理回路に、前記処理結果を出力させるように構成したこと
25 を特徴とする秘密情報の処理プログラム。

7.

請求項 6 記載の秘密情報の処理プログラムにおいて、

前記秘密情報の処理プログラムは、前記秘密情報生成情報として複数の秘密情報部分情報を処理することを特徴とする秘密情報の処理プログラム。

5 ラム。

8.

請求項 6 または 7 記載の秘密情報の処理プログラムにおいて、

前記秘密情報生成情報を他の秘密情報生成情報へ変換する変換手段を
10 さらに備え、

前記秘密情報の処理プログラムは、他の秘密情報生成情報を用いて、
前記処理結果と同一の処理結果を出力することを特徴とする秘密情報の
処理プログラム。

15 9.

請求項 1 ないし 5 いずれかに記載の秘密情報の処理装置を用いて、前記秘密情報を用いた処理結果を送受信する秘密情報の処理システムで
あって、

前記処理結果の受信者側装置は、前記秘密情報生成情報処理手段と前記秘密情報生成情報を、前記処理装置の前記記憶回路に設定する手段
20 を備え、

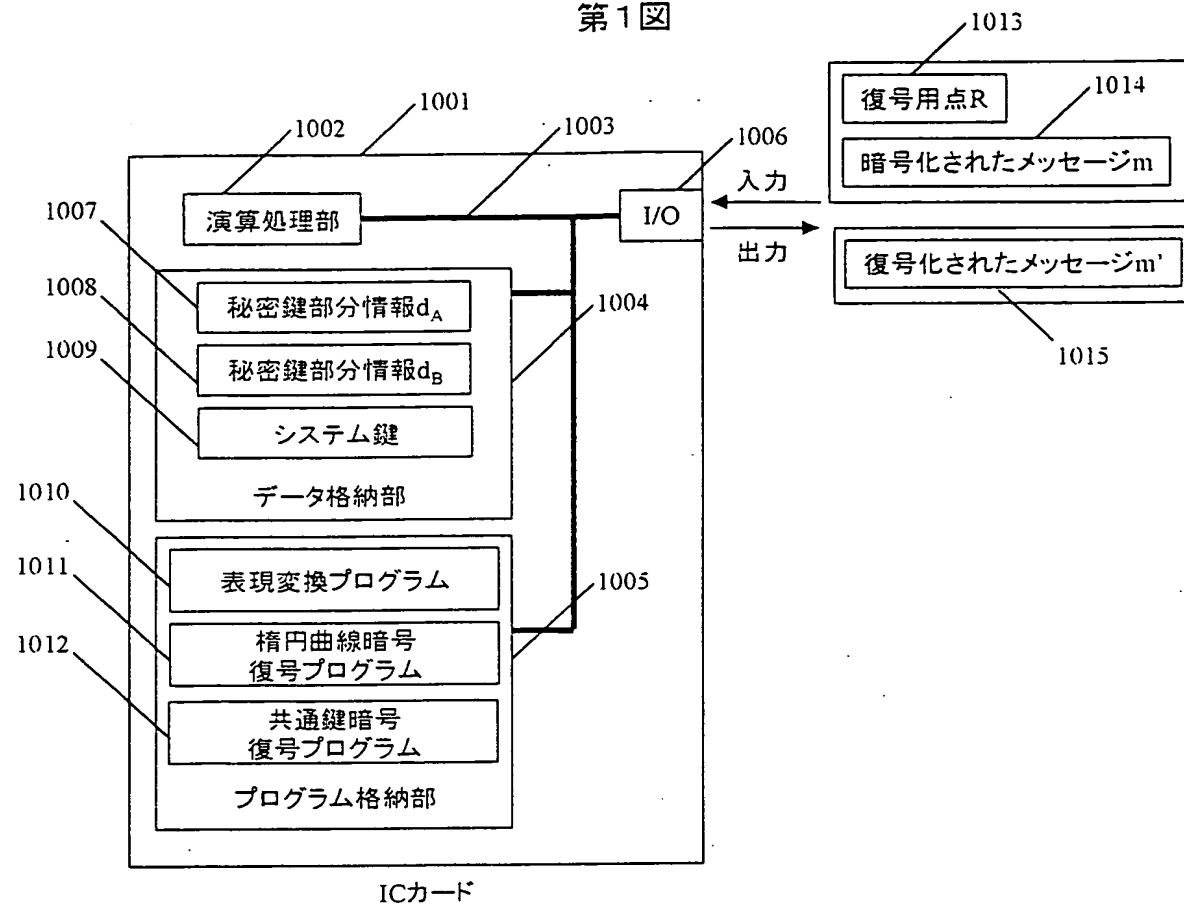
処理装置の使用者側装置は、前記処理装置に処理対象となるデータを
入力する手段と、前記処理装置から前記処理結果を受け取る手段と、前記受け取った処理結果を前記受信者側装置へ送信する手段と
25 を備えることを特徴とする秘密情報の処理システム。

要 約 書

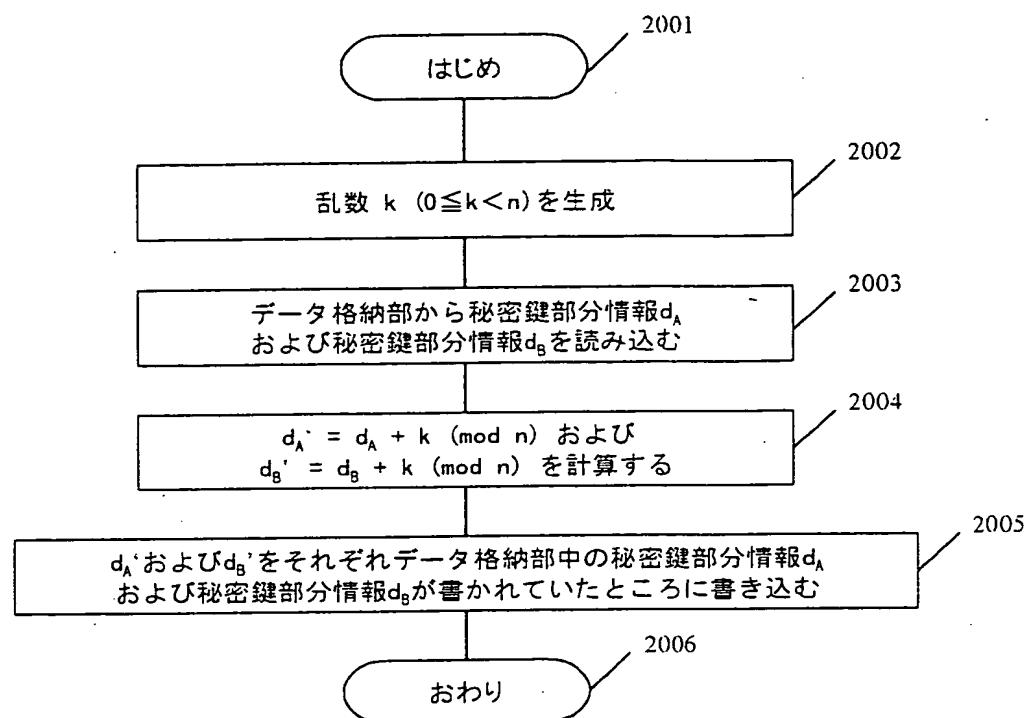
内部に保存した秘密情報の推定するための攻撃方法であるTA(Timing Attack), DPA(Differential Power Analysis), SPA(Simple Power

5 Analysis)などに耐えられるICカードなどの secure cryptographic device を提供するために、内部に保持された秘密情報や、その秘密情報を使った演算を行う時に、その秘密情報や演算中に利用される他の情報を複数の表現方法で表して演算することにより、演算を行うたびごとに演算処理方法が異なるようにし、演算時間や発生する電磁波の強さや消費
10 電流が異なるようにする。

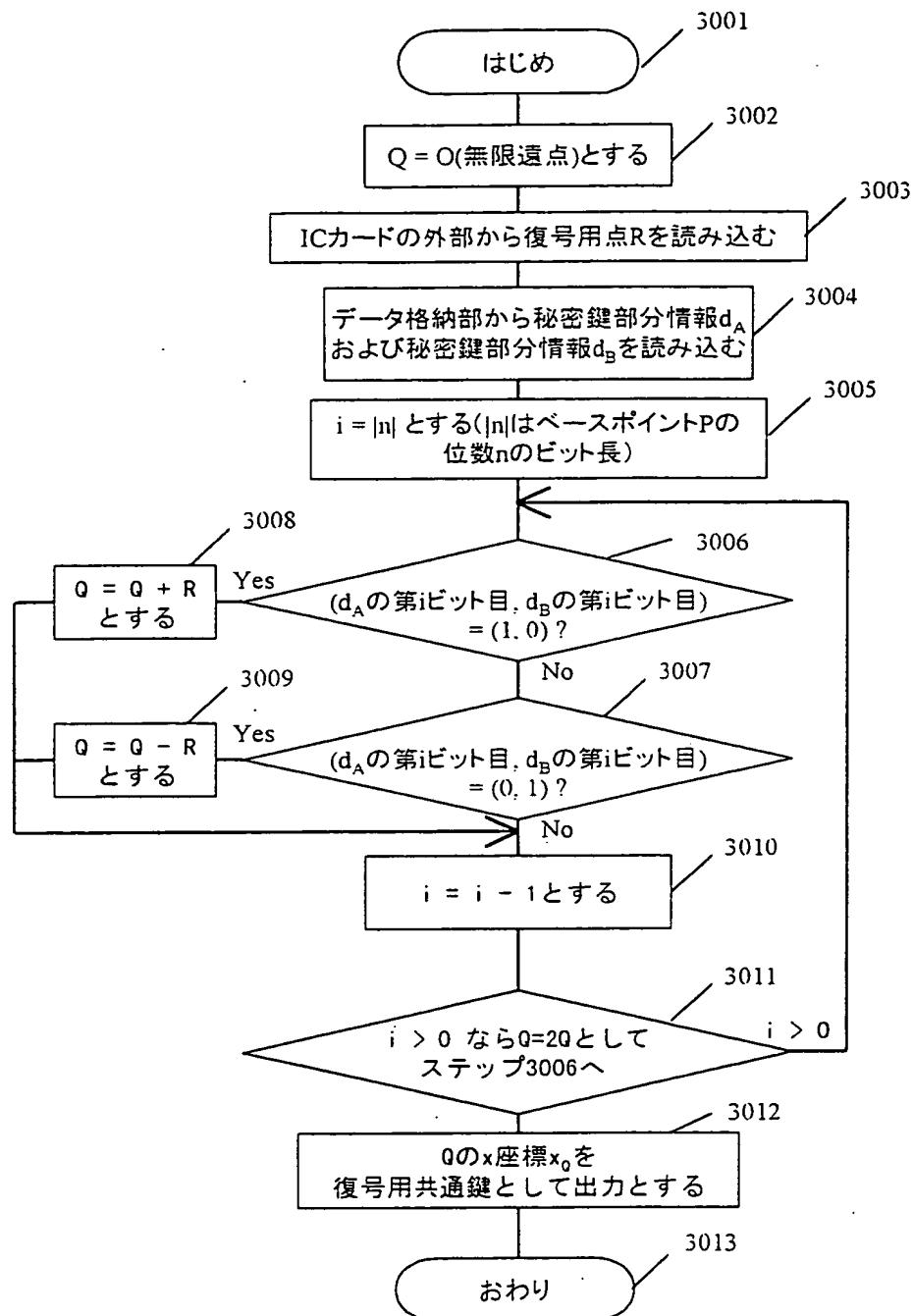
第1図



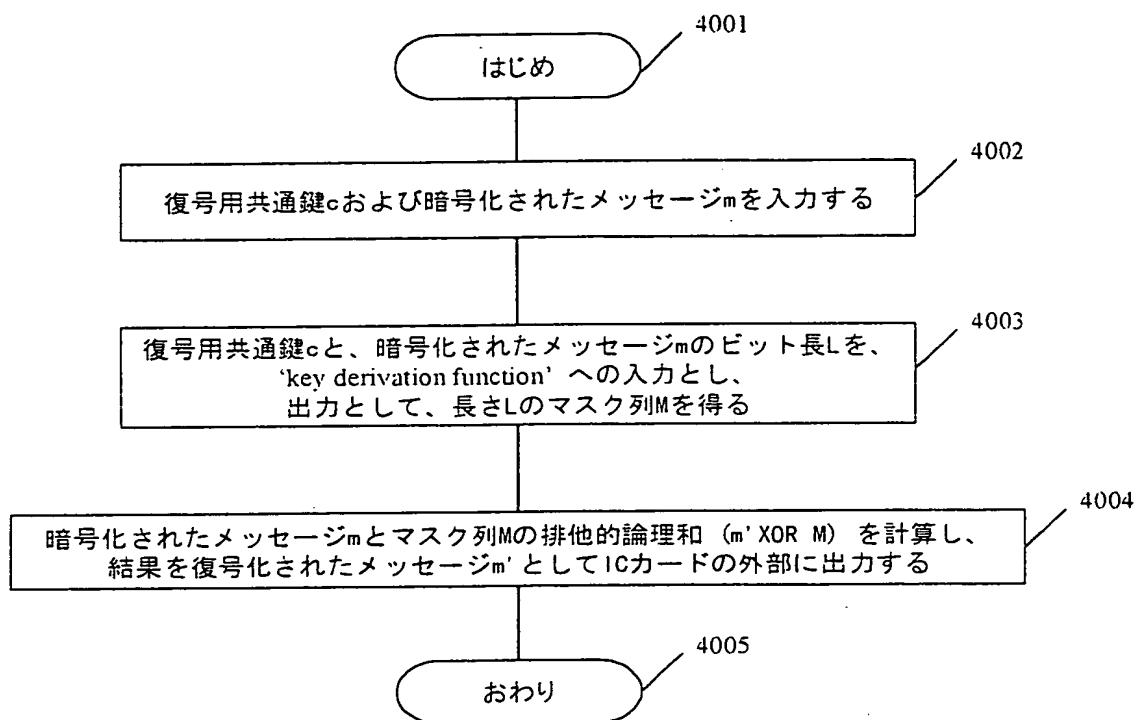
第2図



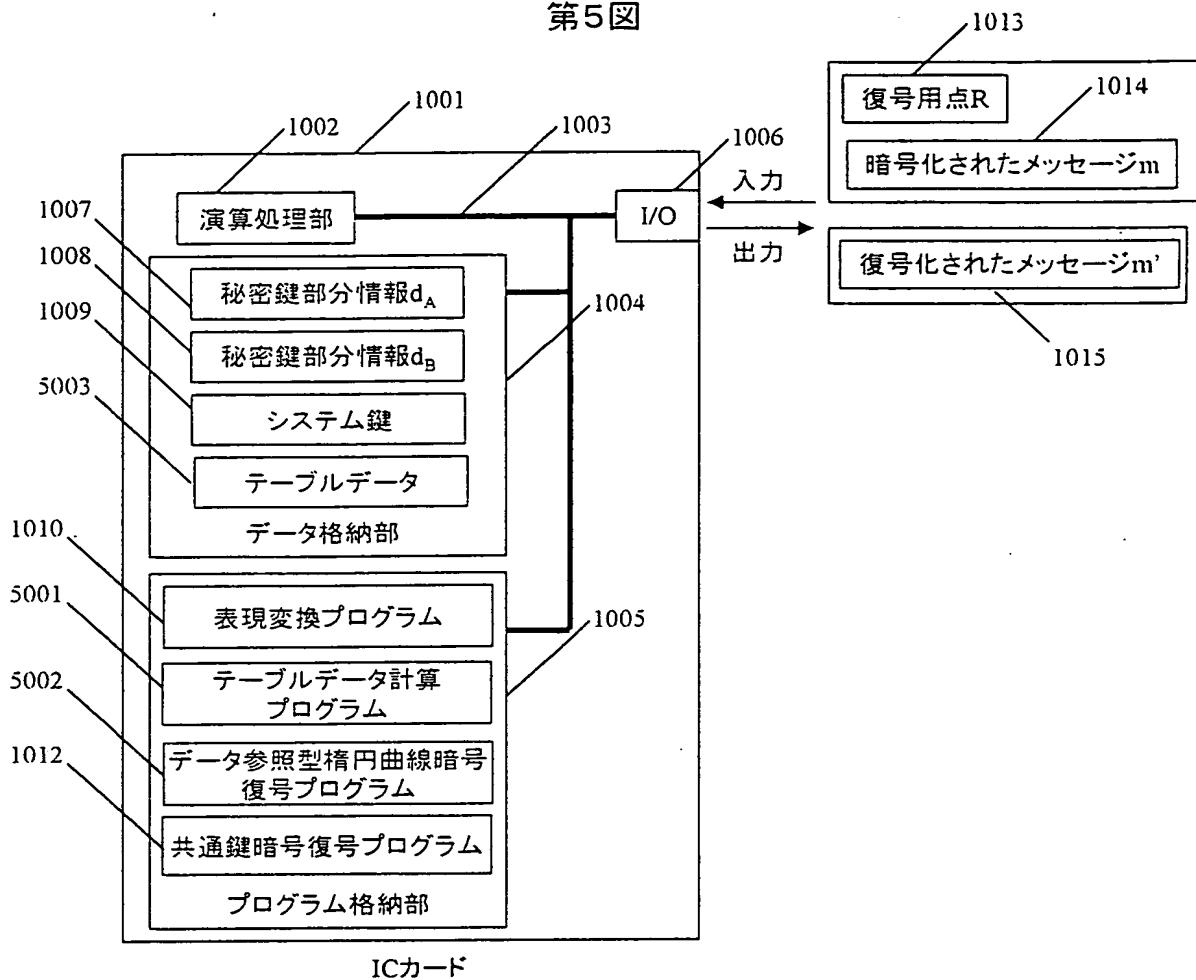
第3図



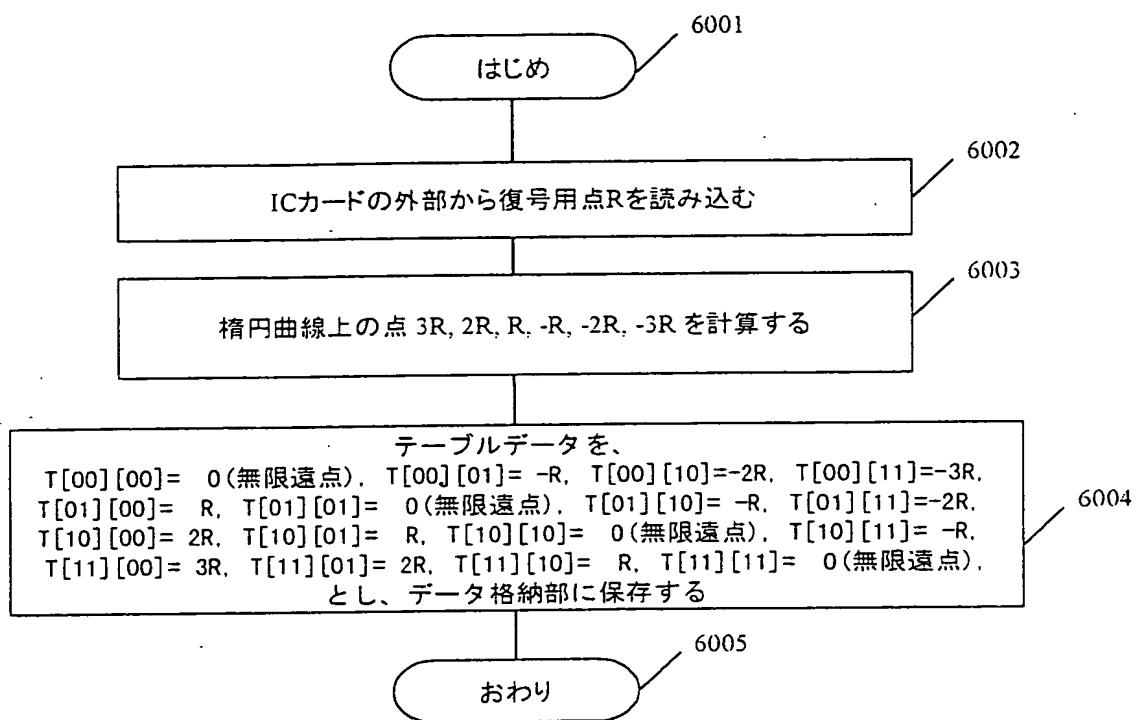
第4図



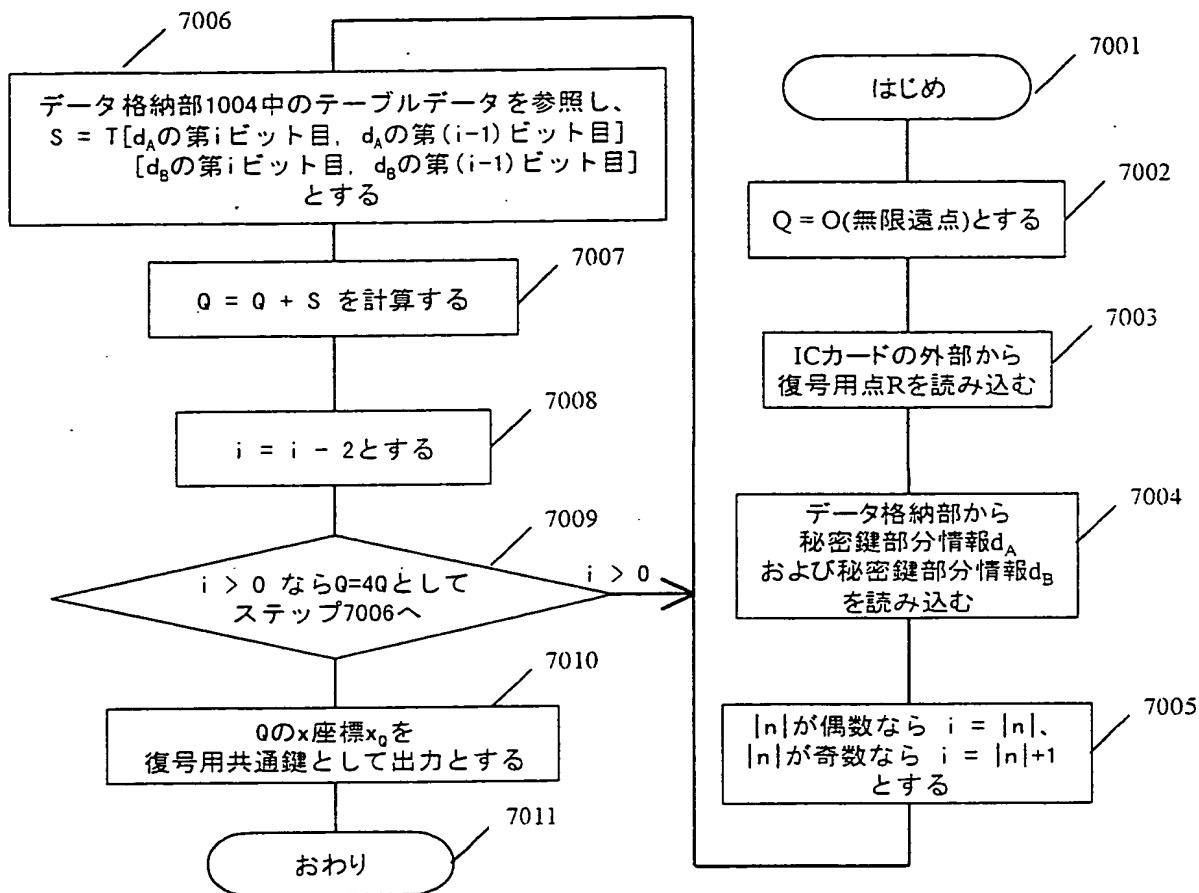
第5図



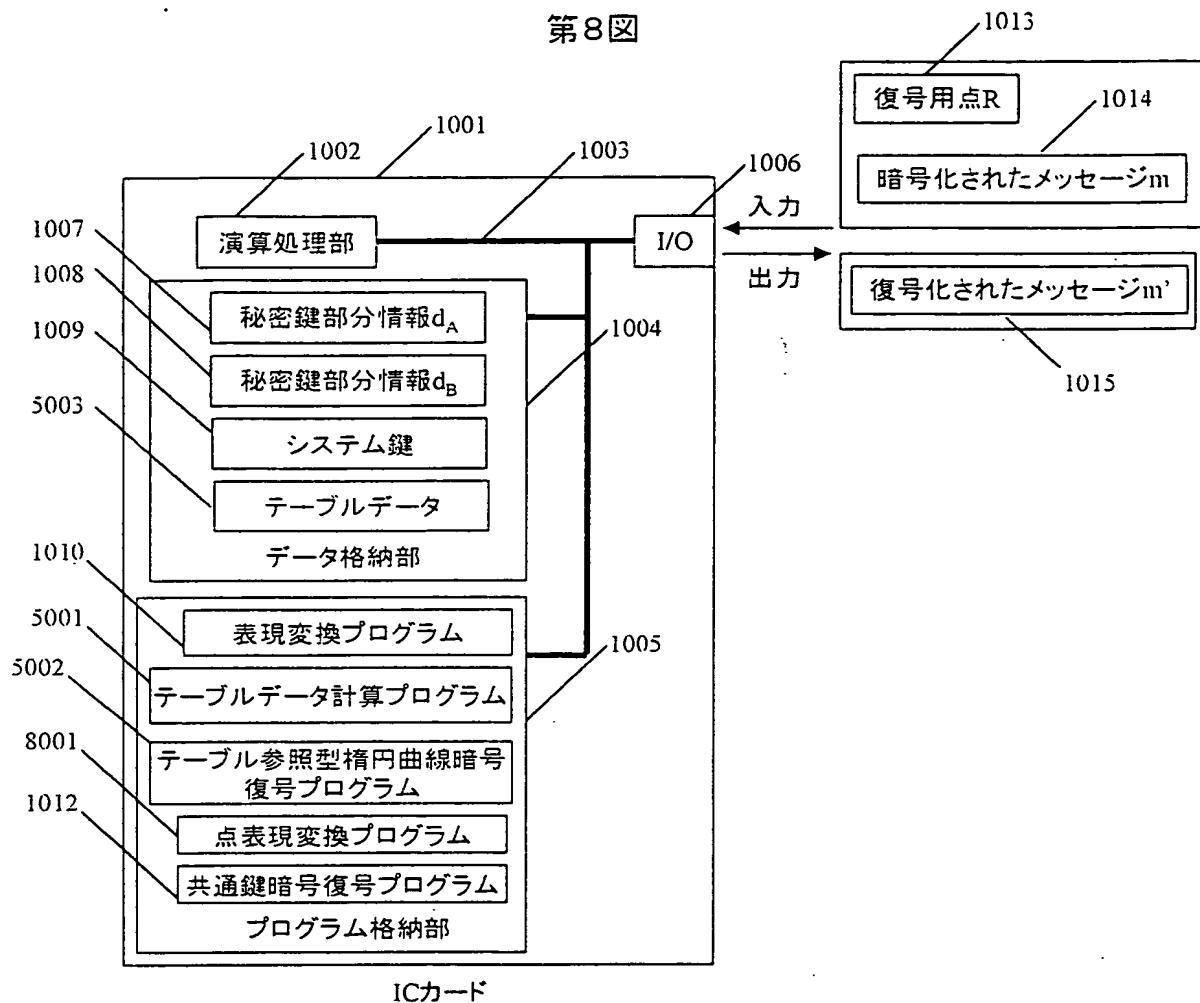
第6図



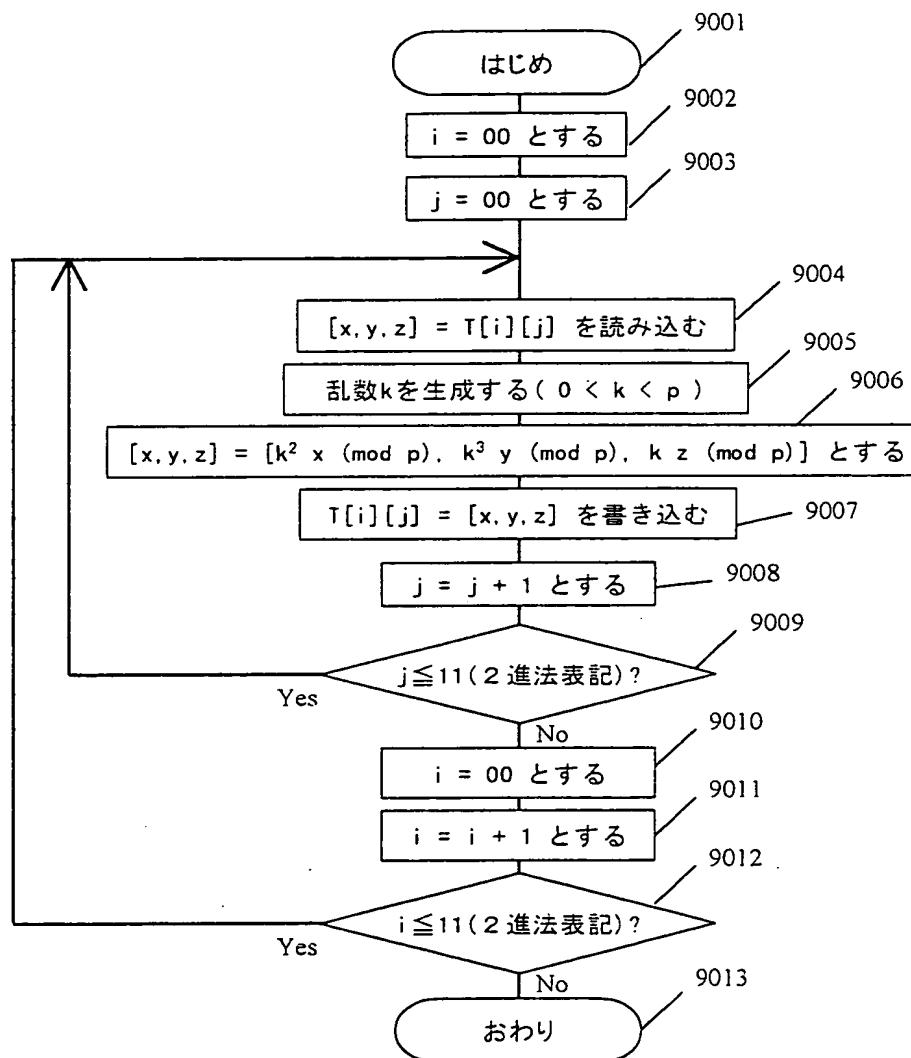
第7図



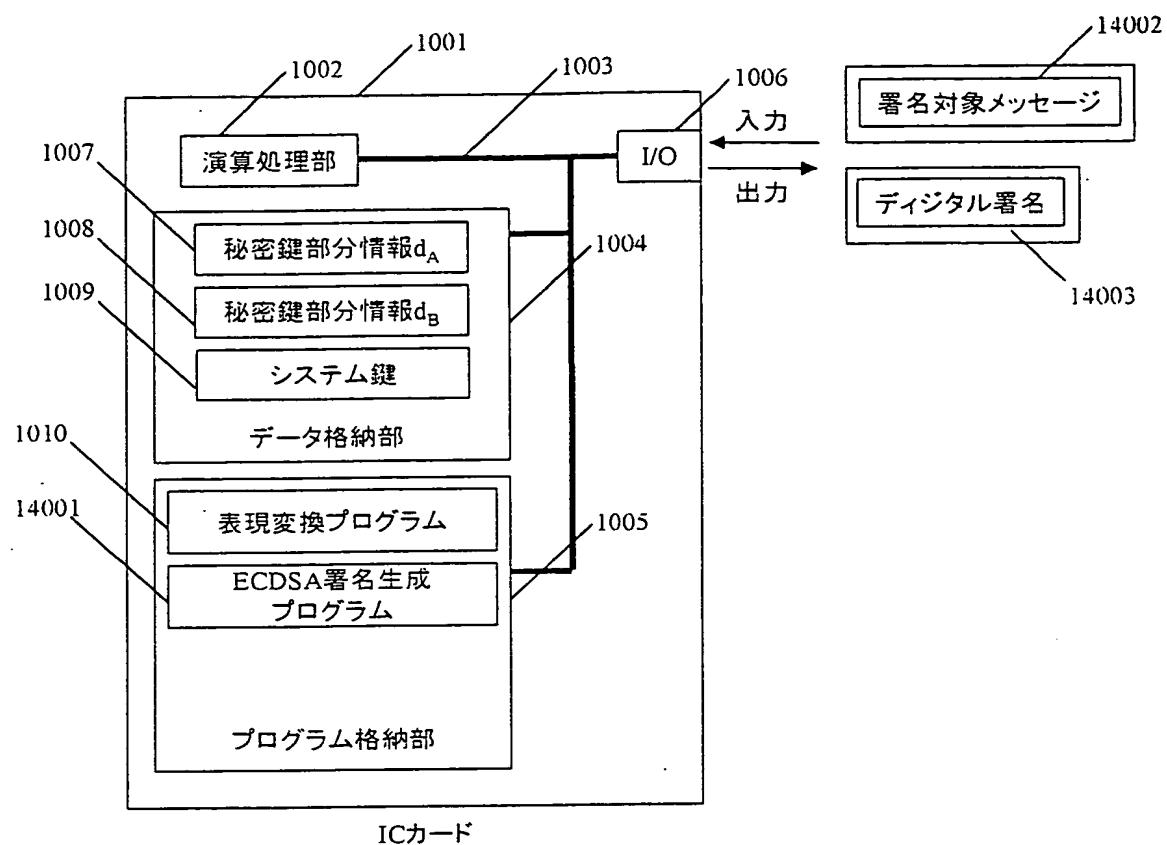
第8図



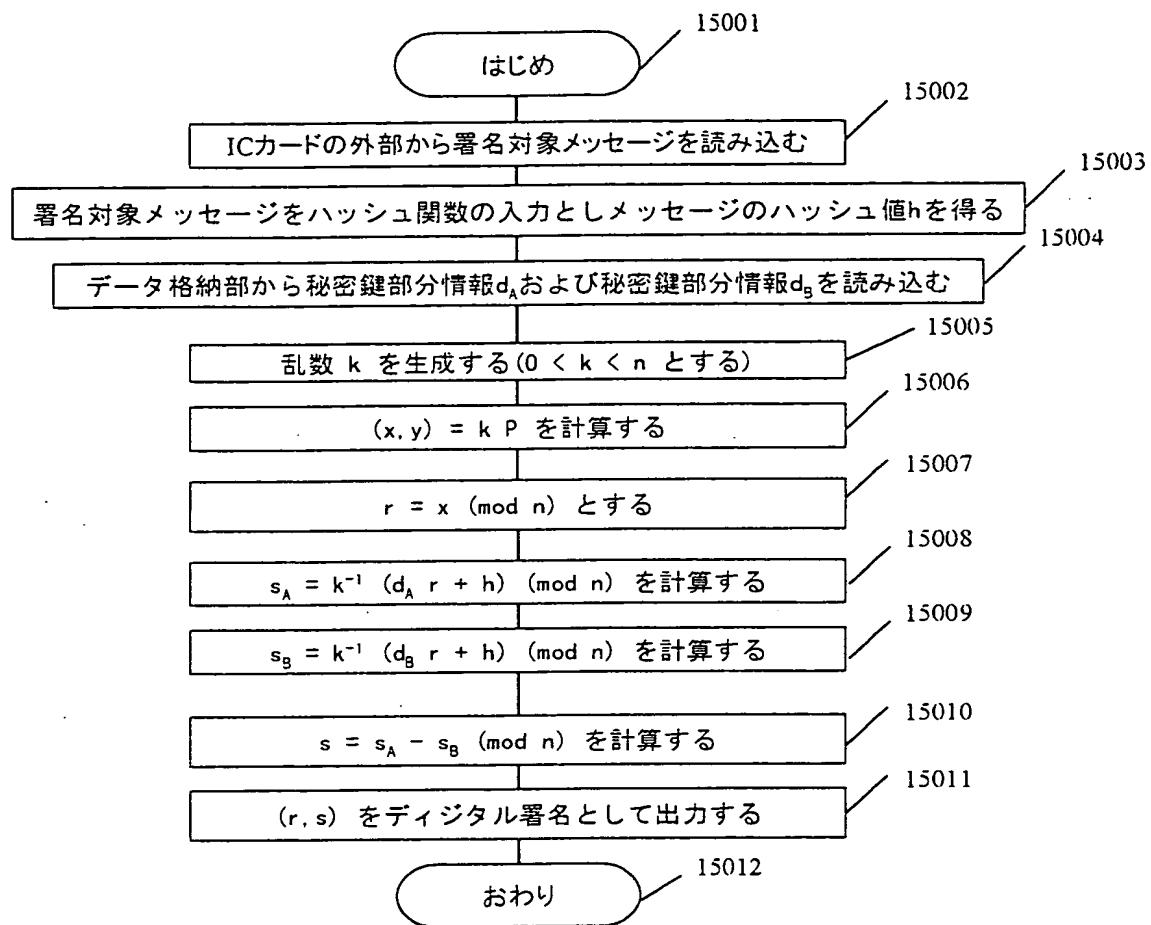
第9図



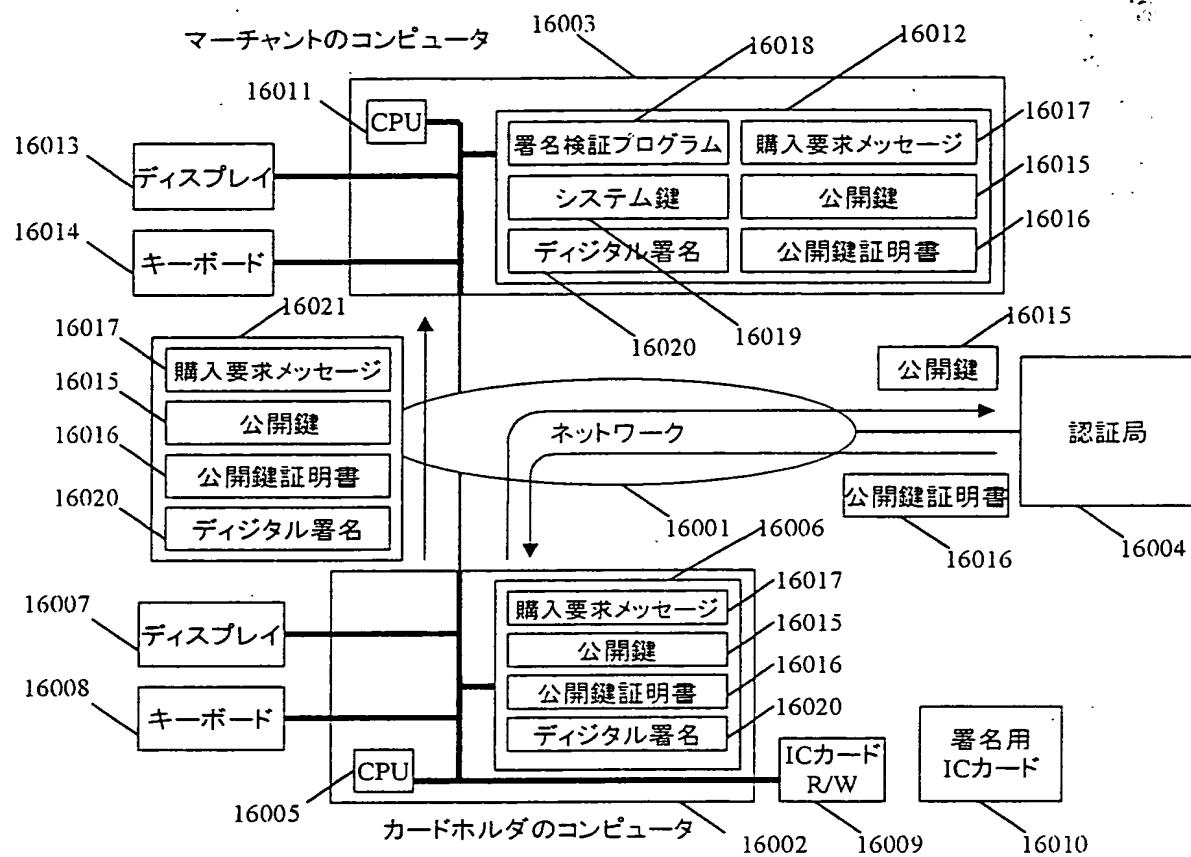
第10図



第11図



第12図



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP99/05353

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl⁷ H04L9/10, G06F12/14, G06K17/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int. Cl⁷ H04L9/10, G06F12/14, G06K17/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-1999**Kokai Jitsuyo Shinan Koho 1971-1999 Jitsuyo Shinan Toroku Koho 1996-1999**

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim-No.
X Y	BRUCE SCHNEIER; APPLIED CRYPTOGRAPHY (SECOND EDITION) John Wiley & Sons, Inc. (1996) "3.7 SECRET SHARING", P.71-73 "3.7 SECRET SHARING", P.71-73	1, 2, 4, 6, 7 3, 5, 8, 9
X Y	JP,10-282881,A (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) 23.Oct.1998 (23.10.98) Full Text, Fig. 1 to Fig. 7 Full Text, Fig. 1 to Fig. 7 (Family: none)	1, 2, 4, 6, 7 3, 5, 8, 9

Further documents are listed in the continuation of Box C.

See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earliest document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

27.12.99

Date of mailing of the international search report

18.01.00

Name and mailing address of the ISA/JP

JAPANESE PATENT OFFICE (ISA/JP)
3-4-3, KASUMIGASEKI, CHIYODA-KU
TOKYO-TO 100-8915 JAPAN

Facsimile No.

Authorized office:

Examiner:

Telephone No. 03-3581-1101 (ex)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP99/05353

C (Continuation).

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP,3-76447,A (SHARP Co., Ltd.) 2. April, 1991 (02.04.91) Page 3, lower right column, line 1-6; Page 3, lower right column, line 13 to page 4, upper left column, line 4; and Page 4, upper right column, line 7-18; and Figs. 1-5 (Family: none)	3, 5, 8, 9
Y	K. Takaragi, et al., "Current Cards Society and Security Technology", The Japanese Society of Printing Science and Technology, Vol. 29, No. 3 (113rd volume) (31.05.92) pp. 288-295	1-9
Y	Yuichi Kaji, et al., Personal Authentication by Password declare-next authentication, -Secure Personal Authentication by Magnetic Card Technical Report of The Institute of Electronics, Information and Communication Engineers (ISEC 95-39 to 44) Vol. 95, No. 423 (15.12.95) Page 21-28	1-9
E, X	JP,11-316542,A (Matsushita Electric Industrial Co., Ltd.) 16 November, 1999 (16.11.99) Full Text, Fig. 1 to Fig. 7 (Family: none)	1-9